



Junos[®] OS

Layer 2 VPNs and VPLS Feature Guide for Routing Devices

Release
15.1



Modified: 2016-11-30

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.

Junos[®] OS Layer 2 VPNs and VPLS Feature Guide for Routing Devices

15.1

Copyright © 2016, 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	xxvii
	Documentation and Release Notes	xxvii
	Supported Platforms	xxvii
	Using the Examples in This Manual	xxvii
	Merging a Full Example	xxviii
	Merging a Snippet	xxviii
	Documentation Conventions	xxix
	Documentation Feedback	xxxi
	Requesting Technical Support	xxxi
	Self-Help Online Tools and Resources	xxxi
	Opening a Case with JTAC	xxxii
Part 1	Common Configuration for All VPNs	
Chapter 1	Overview	3
	Types of VPNs	3
	Layer 2 VPNs	3
	Layer 3 VPNs	4
	VPLS	4
	Virtual-Router Routing Instances	5
	VPNs and Logical Systems	6
	Routers in a VPN	7
	VPN Terminology	7
Chapter 2	Assigning Routing Instances to VPNs	9
	Configuring Routing Instances on PE Routers in VPNs	9
	Configuring the Routing Instance Name for a VPN	10
	Configuring the Description	10
	Configuring the Instance Type	10
	Configuring Interfaces for VPN Routing	11
	General Configuration for VPN Routing	11
	Configuring Interfaces for Layer 3 VPNs	12
	Configuring Interfaces for Carrier-of-Carriers VPNs	12
	Configuring Unicast RPF on VPN Interfaces	13
	Configuring the Route Distinguisher	13
	Configuring Automatic Route Distinguishers	14
	Configuring Virtual-Router Routing Instances in VPNs	14
	Configuring a Routing Protocol Between the Service Provider Routers	15
	Configuring Logical Interfaces Between Participating Routers	15

	Configuring Path MTU Checks for VPN Routing Instances	16
	Enabling Path MTU Checks for a VPN Routing Instance	17
	Assigning an IP Address to the VPN Routing Instance	17
Chapter 3	Distributing Routes in VPNs	19
	Enabling Routing Information Exchange for VPNs	19
	Configuring IBGP Sessions Between PE Routers in VPNs	19
	Configuring Aggregate Labels for VPNs	21
	Configuring a Signaling Protocol and LSPs for VPNs	22
	Using LDP for VPN Signaling	22
	Using RSVP for VPN Signaling	24
	Configuring Policies for the VRF Table on PE Routers in VPNs	25
	Configuring the Route Target	26
	Configuring the Route Origin	26
	Configuring an Import Policy for the PE Router's VRF Table	27
	Configuring an Export Policy for the PE Router's VRF Table	29
	Applying Both the VRF Export and the BGP Export Policies	30
	Configuring a VRF Target	31
	Configuring the Route Origin for VPNs	32
	Configuring the Site of Origin Community on CE Router A	32
	Configuring the Community on CE Router A	33
	Applying the Policy Statement on CE Router A	33
	Configuring the Policy on PE Router D	34
	Configuring the Community on PE Router D	34
	Applying the Policy on PE Router D	34
Chapter 4	Distributing VPN Routes with Target Filtering	37
	Configuring BGP Route Target Filtering for VPNs	37
	BGP Route Target Filtering Overview	37
	Configuring BGP Route Target Filtering for VPNs	38
	Example: BGP Route Target Filtering for VPNs	39
	Example: Configuring BGP Route Target Filtering for VPNs	41
	Configure BGP Route Target Filtering on Router PE1	41
	Configure BGP Route Target Filtering on Router PE2	43
	Configure BGP Route Target Filtering on the Route Reflector	45
	Configure BGP Route Target Filtering on Router PE3	47
	Configuring Static Route Target Filtering for VPNs	49
	Understanding Proxy BGP Route Target Filtering for VPNs	50
	Example: Configuring Proxy BGP Route Target Filtering for VPNs	51
	Example: Configuring an Export Policy for BGP Route Target Filtering for VPNs	66
	Reducing Network Resource Use with Static Route Target Filtering for VPNs . . .	82
Chapter 5	Configuring Forwarding Options for VPNs	83
	Chained Composite Next Hops for Transit Devices for VPNs	83
	Example: Configuring Chained Composite Next Hops for Direct PE-PE Connections in VPNs	85

Chapter 6	Configuring Graceful Restart for VPNs	99
	VPN Graceful Restart	99
	Configuring Graceful Restart for VPNs	100
	Enabling Unicast Reverse-Path Forwarding Check for VPNs	102
	Example: Configuring Unicast Reverse-Path-Forwarding Check	103
	Understanding Unicast Reverse Path Forwarding	103
	Example: Configuring Unicast Reverse-Path-Forwarding Check	103
Chapter 7	Configuring Class of Service for VPNs	113
	VPNs and Class of Service	113
	Rewriting Class of Service Markers and VPNs	113
Chapter 8	Pinging VPNs	115
	Pinging VPNs, VPLS, and Layer 2 Circuits	115
	Setting the Forwarding Class of the Ping Packets	116
	Pinging a VPLS Routing Instance	116
	Pinging a Layer 2 VPN	116
	Pinging a Layer 3 VPN	117
	Pinging a Layer 2 Circuit	117
Part 2	Common Configuration for Layer 2 VPNs and VPLS	
Chapter 9	Overview	121
	Understanding Layer 2 VPNs	121
	Layer 2 VPN Applications	122
	Supported Layer 2 VPN Standards	123
Chapter 10	Layer 2 VPNs Configuration Overview	125
	Introduction to Configuring Layer 2 VPNs	125
	Configuring the Local Site on PE Routers in Layer 2 VPNs	126
	Configuring a Layer 2 VPN Routing Instance	127
	Configuring the Site	127
	Configuring the Remote Site ID	128
	Configuring the Encapsulation Type	129
	Configuring a Site Preference and Layer 2 VPN Multihoming	130
	Tracing Layer 2 VPN Traffic and Operations	131
	Disabling Normal TTL Decrementing for VPNs	132
	Layer 2 VPN Configuration Example	132
	Simple Full-Mesh Layer 2 VPN Overview	132
	Enabling an IGP on the PE Routers	133
	Configuring MPLS LSP Tunnels Between the PE Routers	133
	Configuring IBGP on the PE Routers	134
	Configuring Routing Instances for Layer 2 VPNs on the PE Routers	136
	Configuring CCC Encapsulation on the Interfaces	138
	Configuring VPN Policy on the PE Routers	139
	Layer 2 VPN Configuration Summarized by Router	142
	Summary for Router A (PE Router for Sunnyvale)	142
	Summary for Router B (PE Router for Austin)	144

	Summary for Router C (PE Router for Portland)	146
	Example: Configuring MPLS-Based Layer 2 VPNs	148
	Transmitting Nonstandard BPDUs in Layer 2 VPNs and VPLS	162
Chapter 11	Configuring Layer 2 Interfaces	163
	Configuring CCC Encapsulation for Layer 2 VPNs	163
	Configuring TCC Encapsulation for Layer 2 VPNs and Layer 2 Circuits	164
	Configuring the MTU for Layer 2 Interfaces	165
	Disabling the Control Word for Layer 2 VPNs	167
Chapter 12	Configuring Path Selection for Layer 2 VPNs and VPLS	169
	Understanding BGP Path Selection	169
	Routing Table Path Selection	171
	Effects of Advertising Multiple Paths to a Destination	172
	Enabling BGP Path Selection for Layer 2 VPNs and VPLS	173
	VPLS Path Selection Process for PE Routers	175
Chapter 13	Creating Backup Connections with Redundant Pseudowires	177
	Redundant Pseudowires for Layer 2 Circuits and VPLS	177
	Types of Redundant Pseudowire Configurations	178
	Pseudowire Failure Detection	179
	Configuring Redundant Pseudowires for Layer 2 Circuits and VPLS	179
	Configuring Pseudowire Redundancy on the PE Router	180
	Configuring the Switchover Delay for the Pseudowires	180
	Configuring a Revert Time for the Redundant Pseudowire	181
Chapter 14	Configuring Class of Service for Layer 2 VPNs	183
	Configuring Traffic Policing in Layer 2 VPNs	183
Chapter 15	Monitoring Layer 2 VPNs Using BFD	185
	Configuring BFD for Layer 2 VPN and VPLS	186
	BFD Support for VCCV for Layer 2 VPNs, Layer 2 Circuits, and VPLS	188
	Configuring BFD for VCCV for Layer 2 VPNs, Layer 2 Circuits, and VPLS	188
Part 3	Configuring Group VPNs	
Chapter 16	Configuring Group VPNs	193
	Group VPNv2 Overview	193
	Group VPNv2 Technology Overview	193
	Understanding Group VPNv2	194
	Group VPNv2 and Standard IPsec VPN	194
	Understanding the GDOI Protocol	196
	GDOI Protocol and Group VPNv2	198
	Group VPNv2 Traffic	199
	Group Security Association	199
	Group Controller/Key Server	199
	Group Member	200
	Anti-Replay Protection for Group VPNv2 Traffic	200

	Partial Fail-Open on MX Series Member Routers	200
	Group VPNv2 Implementation Overview	201
	Enabling Group VPNv2	201
	Registering a Group Member	202
	Rekeying a Group Member (groupkey-push Method)	203
	Rekeying a Group Member (groupkey-pull Method)	204
	Authenticating a Group Member	205
	Fragmenting Group VPNv2 Traffic	205
	Encrypting Group VPNv2 Traffic	206
	Decrypting Group VPNv2 Traffic	206
	Configuring a Routing Instance for Group VPNv2	207
	Establishing Multiple Groups, Policies, and SAs	207
	Connecting with Multiple Cooperative GC/KSs	207
	Implementing IP Delivery Delay Detection Protocol (Time-Based Anti-Replay Protection)	207
	Changing Group VPNv2 Configuration	208
	Bypassing Group VPNv2 Configuration	208
	Implementing Partial Fail-open on MX Series Member Routers	208
	Supported GDOI IPsec Parameters	209
	Supported GDOI IKEv1 Parameters	210
	Applying Dynamic Policies	211
	Supporting TOS and DSCP	211
	Interoperability of Group Members	211
	Group VPNv2 Limitations	212
	Configuring Group VPNs in Group VPNv2 on Routing Devices	213
	Example: Configuring Group VPNs in Group VPNv2 on Routing Devices	216
Part 4	Configuring Ethernet VPNs	
Chapter 17	Overview	235
	EVPN Overview	235
	Supported EVPN Standards	236
Chapter 18	Configuring Routing Instances for EVPN	239
	Configuring EVPN Routing Instances	239
	Tracing EVPN Traffic and Operations	242
Chapter 19	Configuring EVPN Multihoming	245
	EVPN Multihoming Overview	245
	Introduction to EVPN Multihoming	245
	Understanding EVPN Multihoming Concepts	247
	EVPN Multihoming Mode of Operation	249
	EVPN Multihoming Implementation	249
	New BGP NLRI	250
	New Extended Communities	252
	New EVPN Route Types	253
	Update to the MAC Forwarding Table	254
	Traffic Flow	255
	Aliasing	256
	Sample Configuration	257

	Designated Forwarder Election	258
	DF Election Roles	258
	DF Election Procedure	259
	DF Election Trigger	259
	DF Election for Virtual Switch	260
	Handling Failover	260
	Configuring EVPN Active-Standby Multihoming	261
	Example: Configuring EVPN Active-Standby Multihoming	264
Chapter 20	Configuring Integrated Bridging and Routing Using EVPNs	297
	EVPN with IRB Solution Overview	298
	Need for an EVPN IRB Solution	298
	Implementing the EVPN IRB Solution	299
	Benefits of Implementing the EVPN IRB Solution	301
	Gateway MAC and IP Synchronization	301
	Layer 3 VPN Interworking	301
	Configuring EVPN with IRB Solution	302
	Example: Configuring EVPN with IRB Solution	304
	EVPN with IRB Solution Overview	305
	Need for an EVPN IRB Solution	305
	Implementing the EVPN IRB Solution	306
	Benefits of Implementing the EVPN IRB Solution	308
	Example: Configuring EVPN with IRB Solution	309
Chapter 21	Configuring EVPN with Support for Virtual Switch	325
	Virtual Switch Support for EVPN Overview	325
	Configuring EVPN with Support for Virtual Switch	327
	Example: Configuring EVPN with Support for Virtual Switch	329
	Virtual Switch Support for EVPN Overview	330
	Example: Configuring EVPN with Support for Virtual Switch	331
Part 5	Configuring Layer 2 Circuits	
Chapter 22	Overview	345
	Layer 2 Circuit Overview	345
Chapter 23	Layer 2 Circuits Configuration Overview	347
	Configuring Static Layer 2 Circuits	347
	Configuring Local Interface Switching in Layer 2 Circuits	348
	Configuring the Interfaces for the Local Interface Switch	348
	Enabling Local Interface Switching When the MTU Does Not Match	349
	Configuring Interfaces for Layer 2 Circuits	350
	Configuring the Address for the Neighbor of the Layer 2 Circuit	350
	Configuring the Neighbor Interface for the Layer 2 Circuit	350
	Configuring a Community for the Layer 2 Circuit	351
	Configuring the Control Word for Layer 2 Circuits	351
	Configuring the Encapsulation Type for the Layer 2 Circuit Neighbor	
	Interface	353
	Enabling the Layer 2 Circuit When the Encapsulation Does Not	
	Match	353

	Configuring the Protect Interface	353
	Configuring the Protect Interface From Switching Over to the Primary Interface	354
	Configuring the Pseudowire Status TLV	354
	Configuring Layer 2 Circuits over Both RSVP and LDP LSPs	355
	Configuring the Virtual Circuit ID	356
	Configuring the Interface Encapsulation Type for Layer 2 Circuits	356
	Configuring ATM2 IQ Interfaces for Layer 2 Circuits	357
	Configuring Policies for Layer 2 Circuits	357
	Configuring the Layer 2 Circuit Community	357
	Configuring the Policy Statement for the Layer 2 Circuit Community	358
	Example: Configuring a Policy for a Layer 2 Circuit Community	359
	Verifying the Layer 2 Circuit Policy Configuration	360
	Configuring LDP for Layer 2 Circuits	360
Chapter 24	Configuring Class of Service with Layer 2 Circuits	361
	Configuring ATM Trunking on Layer 2 Circuits	361
	Layer 2 Circuit Bandwidth Accounting and Call Admission Control	363
	Bandwidth Accounting and Call Admission Control Overview	363
	Selecting an LSP Based on the Bandwidth Constraint	363
	LSP Path Protection and CAC	364
	Secondary Paths and CAC	364
	Fast Reroute and CAC	365
	Link and Node Protection and CAC	365
	Layer 2 Circuits Trunk Mode	365
	Configuring Bandwidth Allocation and Call Admission Control in Layer 2 Circuits	365
Chapter 25	Configuring Pseudowire Redundancy for Layer 2 Circuits	367
	Understanding Pseudowire Redundancy Mobile Backhaul Scenarios	367
	Sample Topology	367
	Benefits of Pseudowire Redundancy Mobile Backhaul	368
	Layer 2 Virtual Circuit Status TLV Extension	368
	How It Works	369
	Example: Configuring Pseudowire Redundancy in a Mobile Backhaul Scenario	371
Chapter 26	Configuring Load Balancing for Layer 2 Circuits	395
	Reducing APS Switchover Time in Layer 2 Circuits	395
	Configuring Per-Packet Load Balancing	396
	Configuring Fast APS Switchover	396
Chapter 27	Configuring Protection Features for Layer 2 Circuits	399
	Egress Protection LSPs for Layer 2 Circuits	399
	Configuring Egress Protection Service Mirroring for BGP Signaled Layer 2 Services	401
	Example: Configuring an Egress Protection LSP for a Layer 2 Circuit	404
	Example: Configuring Layer 2 Circuit Protect Interfaces	415
	Configuring Router PE1	416
	Configuring Router PE2	418

	Configuring Router CE1	419
	Configuring Router CE2	420
	Example: Configuring Layer 2 Circuit Switching Protection	420
Chapter 28	Monitoring Layer 2 Circuits with BFD	433
	Configuring BFD for VCCV for Layer 2 Circuits	433
	Example: Configuring BFD for VCCV for Layer 2 Circuits	435
Chapter 29	Troubleshooting Layer 2 Circuits	443
	Tracing Layer 2 Circuit Operations	443
Part 6	Configuring VPWS VPNs	
Chapter 30	Overview	447
	Understanding VPWS	447
	Supported and Unsupported Features	449
	Supported VPWS Standards	450
	Understanding Multisegment Pseudowire for FEC 129	451
	Understanding Multisegment Pseudowire	451
	Using FEC 129 for Multisegment Pseudowire	452
	Establishing a Multisegment Pseudowire Overview	452
	Pseudowire Status Support for Multisegment Pseudowire	453
	Pseudowire Status Behavior on T-PE	453
	Pseudowire Status Behavior on S-PE	453
	Pseudowire TLV Support for MS-PW	454
	Supported and Unsupported Features	454
Chapter 31	Configuring VPWS VPNs	457
	Understanding FEC 129 BGP Autodiscovery for VPWS	457
	Supported Standards in FEC 129 BGP Autodiscovery for VPWS	457
	Routes and Routing Table Interaction in FEC 129 BGP Autodiscovery for VPWS	457
	Layer 2 VPN Behavior in FEC 129 BGP Autodiscovery for VPWS	458
	BGP Autodiscovery Behavior in FEC 129 BGP Autodiscovery for VPWS ...	459
	LDP Signaling Behavior in VPWS in FEC 129 BGP Autodiscovery for VPWS	459
	Example: Configuring FEC 129 BGP Autodiscovery for VPWS	459
	Example: Configuring MPLS Egress Protection Service Mirroring for BGP Signaled Layer 2 Services	471
	Understanding Multisegment Pseudowire for FEC 129	488
	Understanding Multisegment Pseudowire	488
	Using FEC 129 for Multisegment Pseudowire	489
	Establishing a Multisegment Pseudowire Overview	490
	Pseudowire Status Support for Multisegment Pseudowire	490
	Pseudowire Status Behavior on T-PE	490
	Pseudowire Status Behavior on S-PE	490
	Pseudowire TLV Support for MS-PW	491
	Supported and Unsupported Features	491

	Example: Configuring a Multisegment Pseudowire	492
	Configuring the FAT Flow Label for FEC 128 VPWS Pseudowires for Load-Balancing MPLS Traffic	534
	Configuring the FAT Flow Label for FEC 129 VPWS Pseudowires for Load-Balancing MPLS Traffic	536
Part 7	Configuring VPLS	
Chapter 32	Overview	541
	Introduction to VPLS	541
	Supported VPLS Standards	542
	Supported Platforms and PICs	542
Chapter 33	VPLS Configuration Overview	545
	Introduction to Configuring VPLS	545
	Configuring an Ethernet Switch as the CE Device for VPLS	545
Chapter 34	Configuring Signaling Protocols for VPLS	547
	VPLS Routing and Virtual Ports	547
	BGP Signaling for VPLS PE Routers Overview	549
	Control Word for BGP VPLS Overview	550
	Configuring a Control Word for BGP VPLS	551
	BGP Route Reflectors for VPLS	552
	Interoperability Between BGP Signaling and LDP Signaling in VPLS	554
	LDP-Signaled and BGP-Signaled PE Router Topology	554
	Flooding Unknown Packets Across Mesh Groups	556
	Unicast Packet Forwarding	556
	Configuring Interoperability Between BGP Signaling and LDP Signaling in VPLS	556
	LDP BGP Interworking Platform Support	557
	Configuring FEC 128 VPLS Mesh Groups for LDP BGP Interworking	557
	Configuring FEC 129 VPLS Mesh Groups for LDP BGP Interworking	558
	Configuring Switching Between Pseudowires Using VPLS Mesh Groups	558
	Configuring Integrated Routing and Bridging Support for LDP BGP Interworking with VPLS	559
	Configuring Inter-AS VPLS with MAC Processing at the ASBR	559
	Inter-AS VPLS with MAC Operations Configuration Summary	560
	Configuring the ASBRs for Inter-AS VPLS	560
Chapter 35	Assigning Routing Instances to VPLS	563
	Configuring VPLS Routing Instances	563
	Configuring BGP Signaling for VPLS	564
	Configuring the VPLS Site Name and Site Identifier	565
	Configuring Automatic Site Identifiers for VPLS	566
	Configuring the Site Range	566
	Configuring the VPLS Site Interfaces	568
	Configuring the VPLS Site Preference	569
	Configuring LDP Signaling for VPLS	569
	Configuring LDP Signaling for the VPLS Routing Instance	571
	Configuring LDP Signaling on the Router	572

	Configuring VPLS Routing Instance and VPLS Interface Connectivity	572
	Configuring the VPLS Encapsulation Type	573
	Configuring the VPLS MAC Table Timeout Interval	573
	Configuring the Size of the VPLS MAC Address Table	574
	Limiting the Number of MAC Addresses Learned from an Interface	574
	Removing Addresses from the MAC Address Database	576
	PE Router Mesh Groups for VPLS Routing Instances	576
	Configuring VPLS Fast Reroute Priority	577
	Specifying the VT Interfaces Used by VPLS Routing Instances	579
	Understanding PIM Snooping for VPLS	579
	Example: Configuring PIM Snooping for VPLS	581
	VPLS Label Blocks Operation	591
	Elements of Network Layer Reachability Information	592
	Requirements for NLRI Elements	592
	How Labels are Used in Label Blocks	593
	Label Block Composition	593
	Label Blocks in Junos OS	593
	VPLS Label Block Structure	593
	Configuring the Label Block Size for VPLS	596
	Example: Building a VPLS From Router 1 to Router 3 to Validate Label Blocks . .	596
Chapter 36	Associating Interfaces with VPLS	603
	Configuring Interfaces for VPLS Routing	603
	Configuring the VPLS Interface Name	604
	Configuring VPLS Interface Encapsulation	604
	Enabling VLAN Tagging	606
	Configuring VLAN IDs for Logical Interfaces	607
	Enabling VLANs for Hub and Spoke VPLS Networks	608
	Configuring Aggregated Ethernet Interfaces for VPLS	608
	VPLS and Aggregated Ethernet Interfaces	609
	Enabling VLAN Tagging	610
	Configuring VPLS Without a Tunnel Services PIC	611
Chapter 37	Configuring Pseudowires	613
	Configuring Static Pseudowires for VPLS	613
	VPLS Path Selection Process for PE Routers	615
	BGP and VPLS Path Selection for Multihomed PE Routers	617
	Dynamic Profiles for VPLS Pseudowires	619
	Use Cases for Dynamic Profiles for VPLS Pseudowires	620
	Example: Configuring VPLS Pseudowires with Dynamic Profiles—Basic Solutions	620
	VPLS Pseudowire Interfaces Without Dynamic Profiles	621
	VPLS Pseudowire Interfaces and Dynamic Profiles	622
	CE Routers Without Dynamic Profiles	623

CE Routers and Dynamic Profiles	624
Example: Configuring VPLS Pseudowires with Dynamic Profiles—Complex Solutions	625
Configuration of Routing Instance and Interfaces Without Dynamic Profiles	625
Configuration of Routing Instance and Interfaces Using Dynamic Profiles	626
Configuration of Tag Translation Using Dynamic Profiles	628
Configuring the FAT Flow Label for FEC 128 VPLS Pseudowires for Load-Balancing MPLS Traffic	629
Configuring the FAT Flow Label for FEC 129 VPLS Pseudowires for Load-Balancing MPLS Traffic	631
Example: Configuring H-VPLS BGP-Based and LDP-Based VPLS Interoperation	632
Example: Configuring BGP-Based H-VPLS Using Different Mesh Groups for Each Spoke Router	653
Example: Configuring LDP-Based H-VPLS Using a Single Mesh Group to Terminate the Layer 2 Circuits	675
Example: Configuring H-VPLS With VLANs	681
Example: Configuring H-VPLS Without VLANs	693
Chapter 38 Configuring Multihoming	705
VPLS Multihoming Overview	705
Advantages of Using Autodiscovery for VPLS Multihoming	708
Example: Configuring FEC 129 BGP Autodiscovery for VPWS	708
Understanding VPWS	708
Supported and Unsupported Features	711
Understanding FEC 129 BGP Autodiscovery for VPWS	711
Supported Standards in FEC 129 BGP Autodiscovery for VPWS	711
Routes and Routing Table Interaction in FEC 129 BGP Autodiscovery for VPWS	712
Layer 2 VPN Behavior in FEC 129 BGP Autodiscovery for VPWS	713
BGP Autodiscovery Behavior in FEC 129 BGP Autodiscovery for VPWS	713
LDP Signaling Behavior in VPWS in FEC 129 BGP Autodiscovery for VPWS	713
Example: Configuring FEC 129 BGP Autodiscovery for VPWS	713
Example: Configuring BGP Autodiscovery for LDP VPLS	725
Example: Configuring BGP Autodiscovery for LDP VPLS with User-Defined Mesh Groups	742
VPLS Multihoming Reactions to Network Failures	752
Configuring VPLS Multihoming (FEC 128)	753
VPLS Multihomed Site Configuration	753
Specifying an Interface as the Active Interface	754
Configuring Multihoming on the PE Router	755
VPLS Single-Homed Site Configuration	755

	Example: VPLS Multihoming, Improved Convergence Time	756
	Example: Configuring VPLS Multihoming (FEC 129)	767
	VPLS Multihoming Overview	767
	Example: Configuring VPLS Multihoming (FEC 129)	769
	Next-Generation VPLS for Multicast with Multihoming Overview	781
	Operation of Next-Generation VPLS for Multicast with Multihoming Using BGP	782
	Implementation of Redundancy Using VPLS Multihomed Links Between PE and CE Devices	785
	Example: Next-Generation VPLS for Multicast with Multihoming	787
Chapter 39	Configuring Point-to-Multipoint LSPs	809
	Next-Generation VPLS Point-to-Multipoint Forwarding Overview	809
	Next-Generation VPLS Point-to-Multipoint Forwarding Applications	810
	Implementation	813
	Example: NG-VPLS Using Point-to-Multipoint LSPs	815
	Flooding Unknown Traffic Using Point-to-Multipoint LSPs in VPLS	847
	Configuring Static Point-to-Multipoint Flooding LSPs	849
	Configuring Dynamic Point-to-Multipoint Flooding LSPs	850
	Configuring Dynamic Point-to-Multipoint Flooding LSPs with the Default Template	850
	Configuring Dynamic Point-to-Multipoint Flooding LSPs with a Preconfigured Template	850
	Example: Configuring Ingress Replication for IP Multicast Using MBGP MVPNs	851
	Mapping VPLS Traffic to Specific LSPs	864
Chapter 40	Configuring Inter-AS VPLS and IRB VPLS	867
	Example: Configuring Inter-AS VPLS with MAC Processing at the ASBR	867
	Configuring VPLS and Integrated Routing and Bridging	892
	Configuring MAC Address Flooding and Learning for VPLS	893
	Configuring MSTP for VPLS	894
Chapter 41	Configuring Load Balancing and Performance	895
	Configuring VPLS Load Balancing	895
	Configuring VPLS Load Balancing Based on IP and MPLS Information	897
	Configuring VPLS Load Balancing on MX Series 3D Universal Edge Routers	898
	MAC Moves Loop Prevention in VPLS Network Overview	900
	Configuring VPLS Loop Prevention Due to MAC Moves	901
	Example: Configuring Loop Prevention in VPLS Network Due to MAC Moves	903
	MAC Moves Loop Prevention in VPLS Network Overview	903
	Example: Configuring Loop Prevention in VPLS Network Due to MAC Moves	904
	Configuring Improved VPLS MAC Address Learning on T4000 Routers with Type 5 FPCs	918

Chapter 42	Configuring Class of Service and Firewall Filters in VPLS	921
	Configuring EXP-Based Traffic Classification for VPLS	921
	Configuring Firewall Filters and Policers for VPLS	921
	Configuring a VPLS Filter	922
	Configuring an Interface-Specific Counter for VPLS	923
	Configuring an Action for the VPLS Filter	923
	Configuring VPLS FTFs	923
	Changing Precedence for Spanning-Tree BPDU Packets	923
	Applying a VPLS Filter to an Interface	924
	Applying a VPLS Filter to a VPLS Routing Instance	924
	Configuring a Filter for Flooded Traffic	924
	Configuring a VPLS Policer	925
	Firewall Filter Match Conditions for VPLS Traffic	926
Chapter 43	Monitoring and Tracing VPLS	939
	Configuring Port Mirroring for VPLS Traffic	939
	Configuring Y.1731 Functionality for VPLS to Support Delay and Delay Variation	939
	Tracing VPLS Traffic and Operations	940
Part 8	Connecting Layer 2 VPNs and Circuits to Other VPNs	
Chapter 44	Connecting Layer 2 VPNs to Other VPNs	945
	Layer 2 VPN to Layer 2 VPN Connections	945
	Using the Layer 2 Interworking Interface to Interconnect a Layer 2 VPN to a Layer 2 VPN	945
	Example: Interconnecting a Layer 2 VPN with a Layer 2 VPN	947
	Interconnecting Layer 2 VPNs with Layer 3 VPNs Overview	963
	Interconnecting Layer 2 VPNs with Layer 3 VPNs Applications	963
	Example: Interconnecting a Layer 2 VPN with a Layer 3 VPN	964
Chapter 45	Connecting Layer 2 Circuits to Other VPNs	989
	Using the Layer 2 Interworking Interface to Interconnect a Layer 2 Circuit to a Layer 2 VPN	989
	Applications for Interconnecting a Layer 2 Circuit with a Layer 2 Circuit	990
	Example: Interconnecting a Layer 2 Circuit with a Layer 2 VPN	991
	Example: Interconnecting a Layer 2 Circuit with a Layer 2 Circuit	999
	Applications for Interconnecting a Layer 2 Circuit with a Layer 3 VPN	1015
	Example: Interconnecting a Layer 2 Circuit with a Layer 3 VPN	1015
Part 9	Configuration Statements and Operational Commands	
Chapter 46	Configuration Statements (All VPNs)	1037
	aggregate-label	1038
	backup-neighbor	1039
	description (Routing Instances)	1040
	family route-target	1041
	graceful-restart (Enabling Globally)	1042
	instance-type	1044
	interface (Routing Instances)	1046

	no-forwarding	1047
	proxy-generate	1048
	revert-time (Protocols Layer 2 Circuits)	1049
	route-distinguisher	1051
	route-distinguisher-id	1053
	route-target-filter	1054
	rtf-prefix-list	1055
	switchover-delay	1056
	unicast-reverse-path	1057
	vpn-apply-export	1058
	vrf-export	1059
	vrf-import	1060
	vrf-mtu-check	1061
	vrf-target	1062
Chapter 47	Configuration Statements (Layer 2 VPNs and VPLS)	1065
	action-priority	1069
	active-interface (VPLS Multihoming)	1070
	any (VPLS Multihoming)	1071
	auto-discovery-only	1072
	automatic-site-id	1073
	backup-interface (Layer 2 Circuits)	1074
	bandwidth (Protocols Layer 2 Circuit)	1075
	best-site	1076
	bfd-liveness-detection (Layer 2 VPN and VPLS)	1077
	community (Protocols Layer 2 Circuit)	1078
	connection-protection	1079
	connectivity-type	1080
	control-channel (Protocols OAM)	1081
	control-word (Protocols Layer 2 Circuit Neighbor)	1082
	control-word (Protocols Layer 2 VPN)	1083
	control-word (BGP VPLS)	1084
	description (Protocols Layer 2 Circuit Neighbor)	1084
	description (Protocols Layer 2 VPN)	1085
	detection-time (BFD Liveness Detection)	1086
	encapsulation (Logical Interface)	1088
	encapsulation (Physical Interface)	1092
	encapsulation-type (Layer 2 Circuits)	1097
	encapsulation-type (Layer 2 VPNs)	1099
	egress-protection (Layer 2 circuit)	1100
	egress-protection (MPLS)	1101
	end-interface	1102
	esi	1103
	extended-vlan-list	1104
	family	1105
	family multiservice	1109
	fast-aps-switch	1111
	fast-reroute-priority	1112
	flow-label-receive-static	1113

flow-label-transmit-static	1113
hot-standby	1114
hot-standby (Protocols Layer 2 Circuit)	1115
hot-standby-vc-on (Protocols Layer 2 Circuit)	1116
identifier (VPLS Multihoming for FEC 129)	1117
ignore-encapsulation-mismatch	1118
ignore-mtu-mismatch	1119
interface (EVPN Routing Instances)	1120
interface (Protocols Layer 2 Circuit)	1121
interface (Protocols Layer 2 VPN)	1122
interface (VPLS Multihoming for FEC 129)	1123
interface (VPLS Routing Instances)	1124
interface-mac-limit (VPLS)	1125
install-nexthop	1126
l2circuit	1127
l2ckt	1128
l2vpn	1129
l2vpn (routing-options)	1131
l2vpn-id	1132
l2vpn-use-bgp-rules	1133
label-allocation	1133
label-block-size	1134
label-switched-path-template (Multicast)	1135
local-switching (Layer 2 Circuits)	1136
local-switching (VPLS)	1137
mac-flush	1138
mac-statistics	1140
mac-table-aging-time	1142
mac-table-size	1143
mesh-group (Protocols VPLS)	1144
minimum-interval (BFD Liveness Detection)	1146
minimum-interval (transmit-interval)	1148
minimum-receive-interval (BFD Liveness Detection)	1150
mtu	1152
multiplier (BFD Liveness Detection)	1156
multi-homing (VPLS Multihoming for FEC 128)	1157
multi-homing (VPLS Multihoming for FEC 129)	1158
neighbor (Protocols Layer 2 Circuit)	1159
neighbor (Protocols VPLS)	1161
no-adaptation (BFD Liveness Detection)	1163
no-control-word (BGP VPLS)	1164
no-control-word (Protocols Layer 2 VPN)	1165
no-l2ckt	1166
no-l2vpn	1166
no-local-switching (VPLS)	1167
no-mac-learning	1168
no-revert (Local Switching)	1170
no-revert (Neighbor Interface)	1171
no-tunnel-services	1172

oam	1173
packet-action	1174
peer-active (VPLS Multihoming for FEC 129)	1177
peer-as (VPLS)	1178
ping-interval	1179
policer (Layer 2 VPN)	1180
preference (Interface-Level Preference for VPLS Multihoming for FEC 129)	1181
preference (Site-Level Preference for VPLS Multihoming for FEC 129)	1182
primary (VPLS Multihoming)	1183
protect-interface	1184
protected-l2circuit	1185
protector-interface	1186
protector-pe	1186
proxy (Interfaces)	1187
pseudowire-status-tlv	1187
psn-tunnel-endpoint	1188
remote	1189
remote-site-id	1189
routing-instances	1190
rsvp-te (Routing Instances Provider Tunnel)	1191
send-oam	1191
site (Layer 2 Circuits)	1192
site (VPLS Multihoming for FEC 128)	1193
site (VPLS Multihoming for FEC 129)	1194
site-identifier (Layer 2 Circuits)	1195
site-identifier (VPLS)	1195
site-preference	1196
site-range	1197
source-attachment-identifier (Protocols VPWS)	1198
standby (Protocols Layer 2 Circuit)	1199
static (Protocols Layer 2 Circuit)	1200
static (Protocols VPLS)	1201
static-mac	1202
target-attachment-identifier (Protocols VPWS)	1203
template	1204
threshold (detection-time)	1205
threshold (transmit-interval)	1207
traceoptions (Egress Protection)	1209
traceoptions (Protocols EVPN)	1210
traceoptions (Protocols Layer 2 Circuit)	1212
traceoptions (Protocols Layer 2 VPN)	1214
traceoptions (Protocols VPLS)	1216
transmit-interval (BFD Liveness Detection)	1218
tunnel-services (Routing Instances VPLS)	1220
version (BFD Liveness Detection)	1221
virtual-circuit-id	1222
virtual-mac	1223
vlan-id	1223
vlan-id (routing instance)	1224

	vlan-id-list (Interface in VPLS)	1225
	vlan-tagging	1226
	vpls (Interfaces)	1226
	vpls (Routing Instance)	1227
	vpls-id	1229
	vpls-id-list (protocols vpls mesh-group)	1230
	vpls-mac-move	1231
Chapter 48	Operational Commands	1233
	clear pim snooping join	1235
	clear pim snooping statistics	1237
	clear security group-vpn member ike security-associations	1239
	clear security group-vpn member kek security-associations	1240
	clear vpls mac-address	1241
	clear vpls mac-move-action	1242
	clear vpls mac-table	1243
	ping mpls l2circuit	1244
	ping mpls l2vpn	1247
	ping vpls instance	1250
	request l2circuit-switchover	1252
	show evpn instance	1253
	show interfaces lsi (Label-Switched Interface)	1258
	show l2circuit connections	1261
	show l2vpn connections	1269
	show pim snooping interfaces	1275
	show pim snooping join	1278
	show pim snooping neighbors	1282
	show pim snooping statistics	1287
	show route	1292
	show security group-vpn member ike security-associations	1298
	show security group-vpn member kek security-associations	1301
	show vpls connections	1305
	show vpls flood event-queue	1316
	show vpls flood instance	1318
	show vpls flood route	1320
	show vpls mac-move-action	1322
	show vpls mac-table	1324
	show vpls statistics	1329
Part 10	Index	1335

List of Figures

Part 1	Common Configuration for All VPNs	
Chapter 1	Overview	3
	Figure 1: Logical Interface per Router in a Virtual-Router Routing Instance	6
	Figure 2: Routers in a VPN	7
Chapter 3	Distributing Routes in VPNs	19
	Figure 3: Network Topology of Site of Origin Example	32
Chapter 4	Distributing VPN Routes with Target Filtering	37
	Figure 4: BGP Route Target Filtering Enabled for a Group of VPNs	41
	Figure 5: Proxy BGP Route Target Filtering Topology	52
	Figure 6: BGP Route Target Filtering Export Policy Topology	67
Chapter 5	Configuring Forwarding Options for VPNs	83
	Figure 7: Chained Composite Next Hop for PE-PE Connections	86
Chapter 6	Configuring Graceful Restart for VPNs	99
	Figure 8: Unicast RPF Sample Topoolgy	104
Part 2	Common Configuration for Layer 2 VPNs and VPLS	
Chapter 9	Overview	121
	Figure 9: Layer 2 VPN Connecting CE Routers	122
Chapter 10	Layer 2 VPNs Configuration Overview	125
	Figure 10: Relationship Between the Site Identifier and the Remote Site ID	128
	Figure 11: Example of a Simple Full-Mesh Layer 2 VPN Topology	133
	Figure 12: MPLS-Based Layer 2 VPN	150
Part 3	Configuring Group VPNs	
Chapter 16	Configuring Group VPNs	193
	Figure 13: Standard IPsec VPN and Group VPNv2	195
	Figure 14: Group VPNv2 Using GDOI	198
	Figure 15: Header Preservation	199
	Figure 16: Group Member Rekeying	205
	Figure 17: Group VPN with Single GC/KS	217
	Figure 18: Group VPN with Multiple GC/KS	217
Part 4	Configuring Ethernet VPNs	
Chapter 17	Overview	235
	Figure 19: EVPN Connecting Data Center 1 and Data Center 2	235

Chapter 19	Configuring EVPN Multihoming	245
	Figure 20: CE Device Multihomed to Two PE Routers	247
	Figure 21: Simple EVPN Topology	248
	Figure 22: EVPN Active-Standby Multihoming	266
Chapter 20	Configuring Integrated Bridging and Routing Using EVPNs	297
	Figure 23: Inter-Subnet Traffic Forwarding	300
	Figure 24: Inter-Subnet Traffic Forwarding	307
	Figure 25: EVPN with IRB Solution	310
Chapter 21	Configuring EVPN with Support for Virtual Switch	325
	Figure 26: EVPN with Virtual Switch Support	332
Part 5	Configuring Layer 2 Circuits	
Chapter 22	Overview	345
	Figure 27: Components of a Layer 2 Circuit	345
Chapter 24	Configuring Class of Service with Layer 2 Circuits	361
	Figure 28: ATM Trunking on Layer 2 Circuits	361
Chapter 25	Configuring Pseudowire Redundancy for Layer 2 Circuits	367
	Figure 29: Pseudowire Redundancy Mobile Backhaul Sample Topology	368
	Figure 30: Pseudowire Redundancy Mobile Backhaul Solution	370
	Figure 31: Pseudowire Redundancy in a Mobile Backhaul Example Topology	373
Chapter 27	Configuring Protection Features for Layer 2 Circuits	399
	Figure 32: Egress Protection LSP	400
	Figure 33: Egress Protection LSP Configured from Router PE1 to Router PE2	401
	Figure 34: Egress Protection LSP Configured from Router PE2 to Router PE3	406
	Figure 35: Layer 2 Circuits Using Protect Interfaces	416
	Figure 36: Connection Protection Enabled Between Router PE1 and Router PE2	421
	Figure 37: Connection Protection Using a Pseudowire Configured through Router PE3 as the Protection Path	422
	Figure 38: Connection Protection Using a Pseudowire Configured through Router PE3 as the Working Path	422
Part 6	Configuring VPWS VPNs	
Chapter 30	Overview	447
	Figure 39: VPWS Sample Topology	448
	Figure 40: L2VPN Pseudowire	451
	Figure 41: Multisegment Pseudowire	452
Chapter 31	Configuring VPWS VPNs	457
	Figure 42: Simple VPWS Topology	463
	Figure 43: Egress Protection LSP Configured from Router PE1 to Router PE2	472
	Figure 44: L2VPN Pseudowire	488
	Figure 45: Multisegment Pseudowire	489
	Figure 46: Interarea Multisegment Pseudowire	494
	Figure 47: Inter-AS Multisegment Pseudowire	494

Part 7	Configuring VPLS	
Chapter 34	Configuring Signaling Protocols for VPLS	547
	Figure 48: Flooding a Packet with an Unknown Destination to All PE Routers in the VPLS Instance	548
	Figure 49: BGP and LDP Signaling for a VPLS Routing Instance	555
Chapter 35	Assigning Routing Instances to VPLS	563
	Figure 50: PIM Snooping for VPLS	582
	Figure 51: VPLS Label Block Structure	594
	Figure 52: Label Mapping Example	595
	Figure 53: Router 1 to Router 3 Topology	597
Chapter 37	Configuring Pseudowires	613
	Figure 54: H-VPLS with LDP-Based and BGP-Based VPLS Interoperation	633
	Figure 55: Physical Topology of H-VPLS	654
	Figure 56: Logical Topology of H-VPLS	655
	Figure 57: Physical Topology of H-VPLS using a Single Mesh Group	676
	Figure 58: Basic H-VPLS With One MTU and Two PE-r Devices	682
	Figure 59: Basic H-VPLS With One MTU and Two PE-r Devices	694
Chapter 38	Configuring Multihoming	705
	Figure 60: CE Device Multihomed to Two PE Routers	706
	Figure 61: VPWS Sample Topology	710
	Figure 62: Simple VPWS Topology	718
	Figure 63: BGP Autodiscovery for LDP VPLS	727
	Figure 64: BGP Autodiscovery for LDP VPLS with a User-Defined Mesh Group	743
	Figure 65: VPLS Multihoming Topology with Router PE2 Configured as the Best Site	757
	Figure 66: CE Device Multihomed to Two PE Routers	768
	Figure 67: Topology for FEC 129 Multihoming	771
	Figure 68: Single CE Site Multihomed with Two PE Routers	784
	Figure 69: Two CE Sites Multihomed to a Single PE Router on Different Line Cards	785
	Figure 70: Physical Topology of Next-Generation VPLS for Multicast with Multihoming	788
	Figure 71: Logical Topology of Next-Generation VPLS for Multicast with Multihoming	788
Chapter 39	Configuring Point-to-Multipoint LSPs	809
	Figure 72: Ingress Replication	814
	Figure 73: Point-to-Multipoint Replication	814
	Figure 74: Logical Topology of NG-VPLS Using Point-to-Multipoint LSPs	816
	Figure 75: Physical Topology of NG-VPLS Using Point-to-Multipoint LSPs	817
	Figure 76: Flooding Unknown VPLS Traffic Using Ingress Replication	848
	Figure 77: Flooding Unknown VPLS Traffic Using a Point-to-Multipoint LSP	848
	Figure 78: Internet Multicast Topology	853
Chapter 40	Configuring Inter-AS VPLS and IRB VPLS	867
	Figure 79: Inter-AS VPLS with MAC Operations Example Topology	869

Chapter 41	Configuring Load Balancing and Performance	895
	Figure 80: Example Loop Prevention Due to MAC Move in VPLS Network	906
Part 8	Connecting Layer 2 VPNs and Circuits to Other VPNs	
Chapter 44	Connecting Layer 2 VPNs to Other VPNs	945
	Figure 81: Physical Topology of a Layer 2 VPN to Layer 2 VPN Connection . . .	948
	Figure 82: Logical Topology of a Layer 2 VPN to Layer 2 VPN Connection	948
	Figure 83: Physical Topology of a Layer 2 VPN Terminating into a Layer 3 VPN	966
	Figure 84: Logical Topology of a Layer 2 VPN Terminating into a Layer 3 VPN . .	966
Chapter 45	Connecting Layer 2 Circuits to Other VPNs	989
	Figure 85: Physical Topology of a Layer 2 Circuit to a Layer 2 VPN Connection	992
	Figure 86: Logical Topology of a Layer 2 Circuit to a Layer 2 VPN Connection . .	992
	Figure 87: Physical Topology of a Layer 2 Circuit Terminating into a Layer 2 Circuit	1000
	Figure 88: Logical Topology of a Layer 2 Circuit Terminating into a Layer 2 Circuit	1000
	Figure 89: Physical Topology of a Layer 2 Circuit to Layer 3 VPN Interconnection	1016
	Figure 90: Logical Topology of a Layer 2 Circuit to Layer 3 VPN Interconnection	1016

List of Tables

	About the Documentation	xxvii
	Table 1: Notice Icons	xxix
	Table 2: Text and Syntax Conventions	xxx
Part 2	Common Configuration for Layer 2 VPNs and VPLS	
Chapter 10	Layer 2 VPNs Configuration Overview	125
	Table 3: Local CE Routing Device in the MPLS-Based Layer 2 VPN Topology . . .	150
	Table 4: Remote CE Routing Device in the MPLS-Based Layer 2 VPN Topology	150
	Table 5: Layer 2 VPN Components of the Local PE Routing Device	151
	Table 6: Layer 2 VPN Components of the Remote PE Routing Device	151
Part 3	Configuring Group VPNs	
Chapter 16	Configuring Group VPNs	193
	Table 7: Group VPN vs Traditional Point-to-Point IPsec	196
	Table 8: groupkey-push Message Payloads	197
	Table 9: SA TEK Parameters	209
	Table 10: IKEv1 SA Parameters of Group Member	210
	Table 11: Group VPNv2 Interoperability	212
Part 5	Configuring Layer 2 Circuits	
Chapter 25	Configuring Pseudowire Redundancy for Layer 2 Circuits	367
	Table 12: Pseudowire Status Code for the Pseudowire Status TLV	369
Part 6	Configuring VPWS VPNs	
Chapter 31	Configuring VPWS VPNs	457
	Table 13: Autodiscovery Route Format	458
	Table 14: Pseudowire Route Format	458
Part 7	Configuring VPLS	
Chapter 35	Assigning Routing Instances to VPLS	563
	Table 15: NLRI Elements	592
	Table 16: NLRI Exchange Between for Router 1 and Router 3	597
Chapter 36	Associating Interfaces with VPLS	603
	Table 17: VLAN ID Range by Interface Type	607
	Table 18: VLAN ID Range by Interface Type	610

Chapter 38	Configuring Multihoming	705
	Table 19: Autodiscovery Route Format	712
	Table 20: Pseudowire Route Format	712
	Table 21: Hardware and Software Used	787
Chapter 39	Configuring Point-to-Multipoint LSPs	809
	Table 22: Hardware and Software Used	815
Chapter 42	Configuring Class of Service and Firewall Filters in VPLS	921
	Table 23: Firewall Filter Match Conditions for VPLS Traffic	927
Part 9	Configuration Statements and Operational Commands	
Chapter 48	Operational Commands	1233
	Table 24: show evpn instance Output Fields	1253
	Table 25: Logical Tunnel show interfaces Output Fields	1258
	Table 26: show l2circuit connections Output Fields	1262
	Table 27: show l2vpn connections Output Fields	1270
	Table 28: show pim snooping interface Output Fields	1275
	Table 29: show pim snooping join Output Fields	1278
	Table 30: show pim snooping neighbors Output Fields	1283
	Table 31: show pim snooping statistics Output Fields	1287
	Table 32: show route Output Fields	1293
	Table 33: show security group-vpn member ike security-associations Output Fields	1298
	Table 34: show security group-vpn member kek security-associations	1301
	Table 35: show vpls connections Output Fields	1306
	Table 36: show vpls flood event-queue Output Fields	1316
	Table 37: show vpls flood instance Output Fields	1318
	Table 38: show vpls flood route Output Fields	1320
	Table 39: show vpls mac-move-action Output Fields	1322
	Table 40: show vpls mac-table Output fields	1325
	Table 41: show vpls statistics Output Fields	1329

About the Documentation

- [Documentation and Release Notes on page xxvii](#)
- [Supported Platforms on page xxvii](#)
- [Using the Examples in This Manual on page xxvii](#)
- [Documentation Conventions on page xxix](#)
- [Documentation Feedback on page xxxi](#)
- [Requesting Technical Support on page xxxi](#)

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:

- [ACX Series](#)
- [M Series](#)
- [MX Series](#)
- [PTX Series](#)
- [T 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.xsl;
    }
  }
}
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 [CLI Explorer](#).

Documentation Conventions

[Table 1 on page xxix](#) 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 xxx](#) 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
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<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.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
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.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

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

Convention	Description	Examples
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.
> (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 of the Juniper Networks TechLibrary 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 <http://www.juniper.net/techpubs/feedback/>.
- 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

Common Configuration for All VPNs

- [Overview on page 3](#)
- [Assigning Routing Instances to VPNs on page 9](#)
- [Distributing Routes in VPNs on page 19](#)
- [Distributing VPN Routes with Target Filtering on page 37](#)
- [Configuring Forwarding Options for VPNs on page 83](#)
- [Configuring Graceful Restart for VPNs on page 99](#)
- [Configuring Class of Service for VPNs on page 113](#)
- [Pinging VPNs on page 115](#)

CHAPTER 1

Overview

- [Types of VPNs on page 3](#)
- [VPNs and Logical Systems on page 6](#)
- [Routers in a VPN on page 7](#)
- [VPN Terminology on page 7](#)

Types of VPNs

A virtual private network (VPN) consists of two topological areas: the provider's network and the customer's network. The customer's network is commonly located at multiple physical sites and is also private (non-Internet). A customer site would typically consist of a group of routers or other networking equipment located at a single physical location. The provider's network, which runs across the public Internet infrastructure, consists of routers that provide VPN services to a customer's network as well as routers that provide other services. The provider's network connects the various customer sites in what appears to the customer and the provider to be a private network.

To ensure that VPNs remain private and isolated from other VPNs and from the public Internet, the provider's network maintains policies that keep routing information from different VPNs separate. A provider can service multiple VPNs as long as its policies keep routes from different VPNs separate. Similarly, a customer site can belong to multiple VPNs as long as it keeps routes from the different VPNs separate.

The Junos[®] Operating System (Junos OS) provides several types of VPNs; you can choose the best solution for your network environment. Each of the following VPNs has different capabilities and requires different types of configuration:

- [Layer 2 VPNs on page 3](#)
- [Layer 3 VPNs on page 4](#)
- [VPLS on page 4](#)
- [Virtual-Router Routing Instances on page 5](#)

Layer 2 VPNs

Implementing a Layer 2 VPN on a router is similar to implementing a VPN using a Layer 2 technology such as ATM or Frame Relay. However, for a Layer 2 VPN on a router, traffic is forwarded to the router in Layer 2 format. It is carried by MPLS over the service provider's

network and then converted back to Layer 2 format at the receiving site. You can configure different Layer 2 formats at the sending and receiving sites. The security and privacy of an MPLS Layer 2 VPN are equal to those of an ATM or Frame Relay VPN.

On a Layer 2 VPN, routing occurs on the customer's routers, typically on the CE router. The CE router connected to a service provider on a Layer 2 VPN must select the appropriate circuit on which to send traffic. The PE router receiving the traffic sends it across the service provider's network to the PE router connected to the receiving site. The PE routers do not need to store or process the customer's routes; they only need to be configured to send data to the appropriate tunnel.

For a Layer 2 VPN, customers need to configure their own routers to carry all Layer 3 traffic. The service provider needs to know only how much traffic the Layer 2 VPN needs to carry. The service provider's routers carry traffic between the customer's sites using Layer 2 VPN interfaces. The VPN topology is determined by policies configured on the PE routers.

Layer 3 VPNs

In a Layer 3 VPN, the routing occurs on the service provider's routers. Therefore, Layer 3 VPNs require more configuration on the part of the service provider, because the service provider's PE routers must store and process the customer's routes.

In the Junos OS, Layer 3 VPNs are based on RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*. This RFC defines a mechanism by which service providers can use their IP backbones to provide Layer 3 VPN services to their customers. The sites that make up a Layer 3 VPN are connected over a provider's existing public Internet backbone.

VPNs based on RFC 4364 are also known as BGP/MPLS VPNs because BGP is used to distribute VPN routing information across the provider's backbone, and MPLS is used to forward VPN traffic across the backbone to remote VPN sites.

Customer networks, because they are private, can use either public addresses or private addresses, as defined in RFC 1918, *Address Allocation for Private Internets*. When customer networks that use private addresses connect to the public Internet infrastructure, the private addresses might overlap with the private addresses used by other network users. BGP/MPLS VPNs solve this problem by prefixing a VPN identifier to each address from a particular VPN site, thereby creating an address that is unique both within the VPN and within the public Internet. In addition, each VPN has its own VPN-specific routing table that contains the routing information for that VPN only.

VPLS

Virtual private LAN service (VPLS) allows you to connect geographically dispersed customer sites as if they were connected to the same LAN. In many ways, it works like a Layer 2 VPN. VPLS and Layer 2 VPNs use the same network topology and function similarly. A packet originating within a customer's network is sent first to a CE device. It is then sent to a PE router within the service provider's network. The packet traverses the service provider's network over an MPLS LSP. It arrives at the egress PE router, which then forwards the traffic to the CE device at the destination customer site.

The key difference in VPLS is that packets can traverse the service provider's network in a point-to-multipoint fashion, meaning that a packet originating from a CE device can be broadcast to PE routers in the VPLS. In contrast, a Layer 2 VPN forwards packets in a point-to-point fashion only. The destination of a packet received from a CE device by a PE router must be known for the Layer 2 VPN to function properly.

VPLS is designed to carry Ethernet traffic across an MPLS-enabled service provider network. In certain ways, VPLS mimics the behavior of an Ethernet network. When a PE router configured with a VPLS routing instance receives a packet from a CE device, it first checks the appropriate routing table for the destination of the VPLS packet. If the router has the destination, it forwards it to the appropriate PE router. If it does not have the destination, it broadcasts the packet to all the other PE routers that are members of the same VPLS routing instance. The PE routers forward the packet to their CE devices. The CE device that is the intended recipient of the packet forwards it to its final destination. The other CE devices discard it.

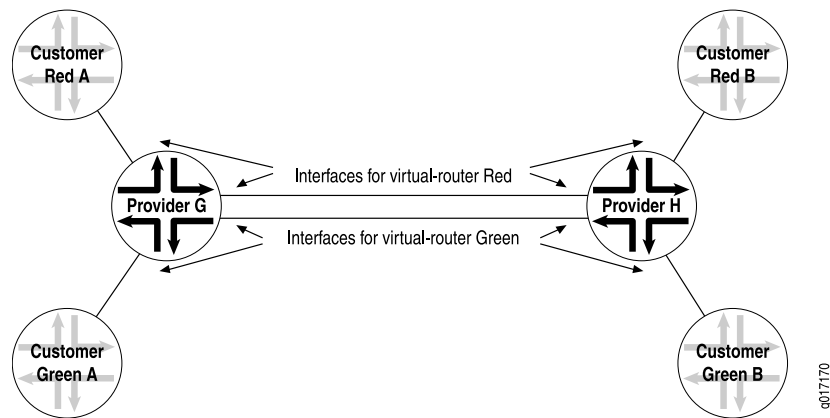
Virtual-Router Routing Instances

A virtual-router routing instance, like a VPN routing and forwarding (VRF) routing instance, maintains separate routing and forwarding tables for each instance. However, many configuration steps required for VRF routing instances are not required for virtual-router routing instances. Specifically, you do not need to configure a route distinguisher, a routing table policy (the **vrf-export**, **vrf-import**, and **route-distinguisher** statements), or MPLS between the P routers.

However, you need to configure separate logical interfaces between each of the service provider routers participating in a virtual-router routing instance. You also need to configure separate logical interfaces between the service provider routers and the customer routers participating in each routing instance. Each virtual-router instance requires its own unique set of logical interfaces to all participating routers.

[Figure 1 on page 6](#) shows how this works. The service provider routers G and H are configured for virtual-router routing instances Red and Green. Each service provider router is directly connected to two local customer routers, one in each routing instance. The service provider routers are also connected to each other over the service provider network. These routers need four logical interfaces: a logical interface to each of the locally connected customer routers and a logical interface to carry traffic between the two service provider routers for each virtual-router instance.

Figure 1: Logical Interface per Router in a Virtual-Router Routing Instance



Layer 3 VPNs do not have this configuration requirement. If you configure several Layer 3 VPN routing instances on a PE router, all the instances can use the same logical interface to reach another PE router. This is possible because Layer 3 VPNs use MPLS (VPN) labels that differentiate traffic going to and from various routing instances. Without MPLS and VPN labels, as in a virtual-router routing instance, you need separate logical interfaces to separate traffic from different instances.

One method of providing this logical interface between the service provider routers is by configuring tunnels between them. You can configure IP Security (IPsec), generic routing encapsulation (GRE), or IP-IP tunnels between the service provider routers, terminating the tunnels at the virtual-router instance.

VPNs and Logical Systems

You can partition a single physical router into multiple logical systems that perform independent routing tasks. Because logical systems perform a subset of the tasks once handled by the physical router, logical systems offer an effective way to maximize the use of a single routing platform.

Logical systems perform a subset of the actions of a physical router and have their own unique routing tables, interfaces, policies, and routing instances. A set of logical systems within a single router can handle the functions previously performed by several small routers.

You can configure Layer 2 VPNs, Layer 3 VPNs, VPLS, and Layer 2 circuits within a logical system. For more information about logical systems, see the *Logical Systems Feature Guide for Routing Devices*.



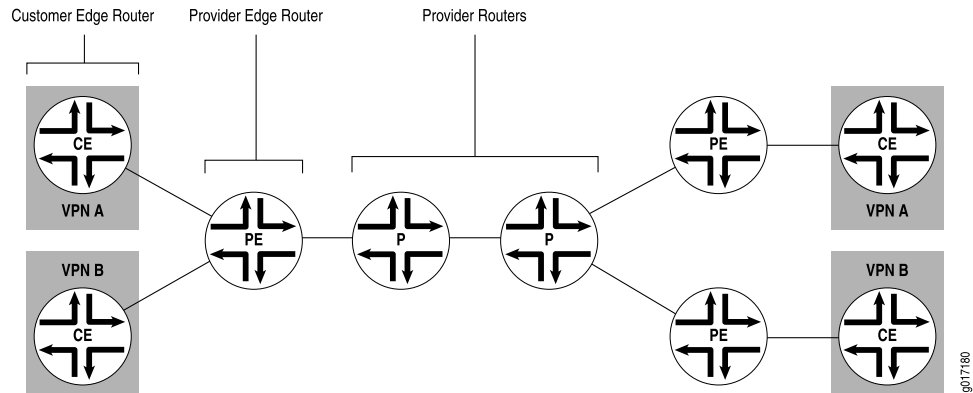
NOTE: Beginning with Junos OS Release 9.3, the logical router feature has been renamed logical system.

All configuration statements, operational commands, show command outputs, error messages, log messages, and SNMP MIB objects that contain the string logical-router or logical-routers have been changed to logical-system and logical-systems, respectively.

Routers in a VPN

Figure 2 on page 7 illustrates how VPN functionality is provided by the provider edge (PE) routers; the provider and customer edge (CE) routers have no special configuration requirements for VPNs.

Figure 2: Routers in a VPN



VPN Terminology

C

Customer edge (CE) devices

Routers or switches located at the customer site that connect to the provider's network. CE devices are typically IP routers, but could also be an Asynchronous Transfer Mode (ATM), Frame Relay, or Ethernet switch.

P

Provider (P) routers

Routers within the core of the provider's network that are not connected to any routers at a customer site but are part of the tunnel between pairs of PE routers. P routers support MPLS LSP or LDP functionality, but do not need to support VPN functionality.

Provider edge (PE) routers

Routers in the provider's network that connect to customer edge devices located at customer sites. PE routers support VPN and label functionality. (The label functionality can be provided either by the Resource Reservation Protocol [RSVP] or Label Distribution Protocol [LDP].) Within a single VPN, pairs of PE routers are connected through a tunnel, which can be either an MPLS label-switched path (LSP) or an LDP tunnel.

CHAPTER 2

Assigning Routing Instances to VPNs

- [Configuring Routing Instances on PE Routers in VPNs on page 9](#)
- [Configuring Virtual-Router Routing Instances in VPNs on page 14](#)
- [Configuring Path MTU Checks for VPN Routing Instances on page 16](#)

Configuring Routing Instances on PE Routers in VPNs

You need to configure a routing instance for each VPN on each of the PE routers participating in the VPN. The configuration procedures outlined in this section are applicable to Layer 2 VPNs, Layer 3 VPNs, and VPLS. The configuration procedures specific to each type of VPN are described in the corresponding sections in the other configuration chapters.

To configure routing instances for VPNs, include the following statements:

```
description text;  
instance-type type;  
interface interface-name;  
route-distinguisher (as-number:number | ip-address:number);  
vrf-import [ policy-names ];  
vrf-export [ policy-names ];  
vrf-target {  
    export community-name;  
    import community-name;  
}
```

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*]**

To configure VPN routing instances, you perform the steps in the following sections:

- [Configuring the Routing Instance Name for a VPN on page 10](#)
- [Configuring the Description on page 10](#)
- [Configuring the Instance Type on page 10](#)
- [Configuring Interfaces for VPN Routing on page 11](#)

- [Configuring the Route Distinguisher on page 13](#)
- [Configuring Automatic Route Distinguishers on page 14](#)

Configuring the Routing Instance Name for a VPN

The name of the routing instance for a VPN can be a maximum of 128 characters and can contain letters, numbers, and hyphens. In Junos OS Release 9.0 and later, you can no longer specify **default** as the actual routing-instance name. You also cannot use any special characters (! @ # \$ % ^ & *, + < > : ;) within the name of a routing instance.



NOTE: In Junos OS Release 9.6 and later, you can include a slash (/) in a routing instance name only if a logical system is not configured. That is, you cannot include the slash character in a routing instance name if a logical system other than the default is explicitly configured.

Specify the routing-instance name with the **routing-instance** statement:

```
routing-instance routing-instance-name {...}
```

You can include this statement at the following hierarchy levels:

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

Configuring the Description

To provide a text description for the routing instance, include the **description** statement. If the text includes one or more spaces, enclose them in quotation marks (" "). Any descriptive text you include is displayed in the output of the **show route instance detail** command and has no effect on the operation of the routing instance.

To configure a text description, include the **description** statement:

```
description text;
```

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 Instance Type

The instance type you configure varies depending on whether you are configuring Layer 2 VPNs, Layer 3 VPNs, VPLS, or virtual routers. Specify the instance type by including the **instance-type** statement:

- To enable Layer 2 VPN routing on a PE router, include the **instance-type** statement and specify the value **l2vpn**:

```
instance-type l2vpn;
```

- To enable VPLS routing on a PE router, include the **instance-type** statement and specify the value **vpls**:

```
instance-type vpls;
```

- Layer 3 VPNs require that each PE router have a VPN routing and forwarding (VRF) table for distributing routes within the VPN. To create the VRF table on the PE router, include the **instance-type** statement and specify the value **vrf**:

```
instance-type vrf;
```



NOTE: Routing Engine based sampling is not supported on VRF routing instances.

- To enable the virtual-router routing instance, include the **instance-type** statement and specify the value **virtual-router**:

```
instance-type virtual-router;
```

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 Interfaces for VPN Routing

On each PE router, you must configure an interface over which the VPN traffic travels between the PE and CE routers.

The sections that follow describe how to configure interfaces for VPNs:

- [General Configuration for VPN Routing on page 11](#)
- [Configuring Interfaces for Layer 3 VPNs on page 12](#)
- [Configuring Interfaces for Carrier-of-Carriers VPNs on page 12](#)
- [Configuring Unicast RPF on VPN Interfaces on page 13](#)

General Configuration for VPN Routing

The configuration described in this section applies to all types of VPNs. For Layer 3 VPNs and carrier-of-carriers VPNs, complete the configuration described in this section before proceeding to the interface configuration sections specific to those topics.

To configure interfaces for VPN routing, include the **interface** statement:

```
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*]

Specify both the physical and logical portions of the interface name, in the following format:

physical.logical

For example, in **at-1/2/1.2**, **at-1/2/1** is the physical portion of the interface name and **2** is the logical portion. If you do not specify the logical portion of the interface name, the value **0** is set by default.

A logical interface can be associated with only one routing instance. If you enable a routing protocol on all instances by specifying **interfaces all** when configuring the master instance of the protocol at the **[edit protocols]** hierarchy level, and if you configure a specific interface for VPN routing at the **[edit routing-instances routing-instance-name]** hierarchy level or at the **[edit logical-systems logical-system-name routing-instances routing-instance-name]** hierarchy level, the latter interface statement takes precedence and the interface is used exclusively for the VPN.

If you explicitly configure the same interface name at the **[edit protocols]** hierarchy level and at either the **[edit routing-instances routing-instance-name]** or **[edit logical-systems logical-system-name routing-instances routing-instance-name]** hierarchy levels, an attempt to commit the configuration fails.

Configuring Interfaces for Layer 3 VPNs

When you configure the Layer 3 VPN interfaces at the **[edit interfaces]** hierarchy level, you must also configure **family inet** when configuring the logical interface:

```
[edit interfaces]
interface-name {
  unit logical-unit-number {
    family inet;
  }
}
```

Configuring Interfaces for Carrier-of-Carriers VPNs

When you configure carrier-of-carriers VPNs, you need to configure the **family mpls** statement in addition to the **family inet** statement for the interfaces between the PE and CE routers. For carrier-of-carriers VPNs, configure the logical interface as follows:

```
[edit interfaces]
interface-name {
  unit logical-unit-number {
    family inet;
    family mpls;
  }
}
```

If you configure **family mpls** on the logical interface and then configure this interface for a non-carrier-of-carriers routing instance, the **family mpls** statement is automatically removed from the configuration for the logical interface, since it is not needed.

Configuring Unicast RPF on VPN Interfaces

For VPN interfaces that carry IP version 4 or version 6 (IPv4 or IPv6) traffic, you can reduce the impact of denial-of-service (DoS) attacks by configuring unicast reverse path forwarding (RPF). Unicast RPF helps determine the source of attacks and rejects packets from unexpected source addresses on interfaces where unicast RPF is enabled.

You can configure unicast RPF on a VPN interface by enabling unicast RPF on the interface and including the **interface** statement at the **[edit routing-instances routing-instance-name]** hierarchy level.

You cannot configure unicast RPF on the core-facing interfaces. You can only configure unicast RPF on the CE router-to-PE router interfaces on the PE router. However, for virtual-router routing instances, unicast RPF is supported on all interfaces you specify in the routing instance.

For information about how to configure unicast RPF on VPN interfaces, see *Configuring Unicast RPF*.

Configuring the Route Distinguisher

Each routing instance that you configure on a PE router must have a unique route distinguisher associated with it. VPN routing instances need a route distinguisher to help BGP to distinguish between potentially identical network layer reachability information (NLRI) messages received from different VPNs. If you configure different VPN routing instances with the same route distinguisher, the commit fails.

For Layer 2 VPNs and VPLS, if you have configured the **l2vpn-use-bgp-rules** statement, you must configure a unique route distinguisher for each PE router participating in a specific routing instance.

For other types of VPNs, we recommend that you use a unique route distinguisher for each PE router participating in the routing instance. Although you can use the same route distinguisher on all PE routers for the same VPN routing instance (except for Layer 2 VPNs and VPLS), if you use a unique route distinguisher, you can determine the CE router from which a route originated within the VPN.

To configure a route distinguisher on a PE router, include the **route-distinguisher** statement:

```
route-distinguisher (as-number:number | ip-address:number);
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

The route distinguisher is a 6-byte value that you can specify in one of the following formats:

- **as-number:number**, where **as-number** is an autonomous system (AS) number (a 2-byte value) and **number** is any 4-byte value. The AS number can be in the range 1 through 65,535. We recommend that you use an Internet Assigned Numbers Authority (IANA)-assigned, nonprivate AS number, preferably the Internet service provider's (ISP's) own or the customer's own AS number.

- ***ip-address:number***, where ***ip-address*** is an IP address (a 4-byte value) and ***number*** is any 2-byte value. The IP address can be any globally unique unicast address. We recommend that you use the address that you configure in the **router-id** statement, which is a nonprivate address in your assigned prefix range.

Configuring Automatic Route Distinguishers

If you configure the **route-distinguisher-id** statement at the **[edit routing-options]** hierarchy level, a route distinguisher is automatically assigned to the routing instance. If you also configure the **route-distinguisher** statement in addition to the **route-distinguisher-id** statement, the value configured for **route-distinguisher** supersedes the value generated from **route-distinguisher-id**.

To assign a route distinguisher automatically, include the **route-distinguisher-id** statement:

```
route-distinguisher-id ip-address;
```

You can include this statement at the following hierarchy levels:

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

A type 1 route distinguisher is automatically assigned to the routing instance using the format ***ip-address:number***. The IP address is specified by the **route-distinguisher-id** statement and the number is unique for the routing instance.

Related Documentation

- [Configuring Policies for the VRF Table on PE Routers in VPNs on page 25](#)
- [Configuring BGP Route Target Filtering for VPNs on page 37](#)

Configuring Virtual-Router Routing Instances in VPNs

A virtual-router routing instance, like a VRF routing instance, maintains separate routing and forwarding tables for each instance. However, many of the configuration steps required for VRF routing instances are not required for virtual-router routing instances. Specifically, you do not need to configure a route distinguisher, a routing table policy (the **vrf-export**, **vrf-import**, and **route-distinguisher** statements), or MPLS between the service provider routers.

Configure a virtual-router routing instance by including the following statements:

```
description text;  
instance-type virtual-router;  
interface interface-name;  
protocols { ... }
```

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*]**

The following sections explain how to configure a virtual-router routing instance:

- [Configuring a Routing Protocol Between the Service Provider Routers on page 15](#)
- [Configuring Logical Interfaces Between Participating Routers on page 15](#)

Configuring a Routing Protocol Between the Service Provider Routers

The service provider routers need to be able to exchange routing information. You can configure the following protocols for the virtual-router routing instance **protocols** statement configuration at the **[edit routing-instances routing-instance-name]** hierarchy level:

- BGP
- IS-IS
- LDP
- OSPF
- Protocol Independent Multicast (PIM)
- RIP

You can also configure static routes.

IBGP route reflection is not supported for virtual-router routing instances.

If you configure LDP under a virtual-router instance, LDP routes are placed by default in the routing instance's inet.0 and inet.3 routing tables (for example, sample.inet.0 and sample.inet.3). To restrict LDP routes to only the routing instance's inet.3 table, include the **no-forwarding** statement:

no-forwarding;

You can include this statement at the following hierarchy levels:

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

When you restrict the LDP routes to only the inet.3 routing table, the corresponding IGP route in the inet.0 routing table can be redistributed and advertised into other routing protocols.

For information about routing tables, see *Understanding Junos OS Routing Tables*.

Configuring Logical Interfaces Between Participating Routers

You must configure an interface to each customer router participating in the routing instance and to each P router participating in the routing instance. Each virtual-router routing instance requires its own separate logical interfaces to all P routers participating in the instance. To configure interfaces for virtual-router instances, include the **interface** statement:

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*]**

Specify both the physical and logical portions of the interface name, in the following format:

physical.logical

For example, in **at-1/2/1.2**, **at-1/2/1** is the physical portion of the interface name and **2** is the logical portion. If you do not specify the logical portion of the interface name, **0** is set by default.

You must also configure the interfaces at the **[edit interfaces]** hierarchy level.

One method of providing this logical interface between the provider routers is by configuring tunnels between them. You can configure IP Security (IPsec), generic routing encapsulation (GRE), or IP-IP tunnels between the provider routers, terminating the tunnels at the virtual-router instance.

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

Configuring Path MTU Checks for VPN Routing Instances

By default, the maximum transmission unit (MTU) check for VPN routing instances is disabled on M Series routers (except the M320 router) and enabled for the M320 router and T Series routers. On M Series routers, you can configure path MTU checks on the outgoing interfaces for unicast traffic routed on VRF routing instances and on virtual-router routing instances.

When you enable an MTU check, the routing platform sends an Internet Control Message Protocol (ICMP) message when a packet traversing the routing instance exceeds the MTU size and has the **do-not-fragment** bit set. The ICMP message uses the VRF local address as its source address.

For an MTU check to work in a routing instance, you must both include the **vrf-mtu-check** statement at the **[edit chassis]** hierarchy level and assign at least one interface containing an IP address to the routing instance.

For more information about the path MTU check, see the *Junos OS Administration Library for Routing Devices*.

To configure path MTU checks, do the tasks described in the following sections:

- [Enabling Path MTU Checks for a VPN Routing Instance on page 17](#)
- [Assigning an IP Address to the VPN Routing Instance on page 17](#)

Enabling Path MTU Checks for a VPN Routing Instance

To enable path checks on the outgoing interface for unicast traffic routed on a VRF or virtual-router routing instance, include the **vrf-mtu-check** statement at the **[edit chassis]** hierarchy level:

```
[edit chassis]  
vrf-mtu-check;
```

Assigning an IP Address to the VPN Routing Instance

To ensure that the path MTU check functions properly, at least one IP address must be associated with each VRF or virtual-router routing instance. If an IP address is not associated with the routing instance, ICMP reply messages cannot be sent.

Typically, the VRF or virtual-router routing instance IP address is drawn from among the IP addresses associated with interfaces configured for that routing instance. If none of the interfaces associated with a VRF or virtual-router routing instance is configured with an IP address, you need to explicitly configure a logical loopback interface with an IP address. This interface must then be associated with the routing instance. See *Configuring Logical Units on the Loopback Interface for Routing Instances in Layer 3 VPNs* for details.

CHAPTER 3

Distributing Routes in VPNs

- [Enabling Routing Information Exchange for VPNs on page 19](#)
- [Configuring IBGP Sessions Between PE Routers in VPNs on page 19](#)
- [Configuring Aggregate Labels for VPNs on page 21](#)
- [Configuring a Signaling Protocol and LSPs for VPNs on page 22](#)
- [Configuring Policies for the VRF Table on PE Routers in VPNs on page 25](#)
- [Configuring the Route Origin for VPNs on page 32](#)

Enabling Routing Information Exchange for VPNs

For Layer 2 VPNs, Layer 3 VPNs, virtual-router routing instances, VPLS, EVPNs, and Layer 2 circuits to function properly, the service provider's PE and P routers must be able to exchange routing information. For this to happen, you must configure either an IGP (such as OSPF or IS-IS) or static routes on these routers. You configure the IGP on the master instance of the routing protocol process at the **[edit protocols]** hierarchy level, not within the routing instance used for the VPN—that is, not at the **[edit routing-instances]** hierarchy level.

When you configure the PE router, do not configure any summarization of the PE router's loopback addresses at the area boundary. Each PE router's loopback address should appear as a separate route.

Related Documentation

- *Example: Configuring IS-IS*
- *Examples: Configuring Static Routes*
- *OSPF Feature Guide for Routing Devices*

Configuring IBGP Sessions Between PE Routers in VPNs

You must configure an IBGP session between the PE routers to allow the PE routers to exchange information about routes originating and terminating in the VPN. The PE routers rely on this information to determine which labels to use for traffic destined for remote sites.

Configure an IBGP session for the VPN as follows:

[edit protocols]

```
bgp {
  group group-name {
    type internal;
    local-address ip-address;
    family evpn {
      signaling;
    }
    family (inet-vpn | inet6-vpn) {
      unicast;
    }
    family l2vpn {
      signaling;
    }
    neighbor ip-address;
  }
}
```

The IP address in the **local-address** statement is the address of the loopback interface on the local PE router. The IBGP session for the VPN runs through the loopback address. (You must also configure the loopback interface at the **[edit interfaces]** hierarchy level.)

The IP address in the **neighbor** statement is the loopback address of the neighboring PE router. If you are using RSVP signaling, this IP address is the same address you specify in the **to** statement at the **[edit mpls label-switched-path *lsp-path-name*]** hierarchy level when you configure the MPLS LSP.

The **family** statement allows you to configure the IBGP session for Layer 2 VPNs, VPLS, EVPNs or for Layer 3 VPNs.

- To configure an IBGP session for Layer 2 VPNs and VPLS, include the **signaling** statement at the **[edit protocols bgp group *group-name* family l2vpn]** hierarchy level:

```
[edit protocols bgp group group-name family l2vpn]
signaling;
```

- To configure an IBGP session for EVPNs, include the **signaling** statement at the **[edit protocols bgp group *group-name* family evpn]** hierarchy level:

```
[edit protocols bgp group group-name family evpn]
signaling;
```

- To configure an IPv4 IBGP session for Layer 3 VPNs, configure the **unicast** statement at the **[edit protocols bgp group *group-name* family inet-vpn]** hierarchy level:

```
[edit protocols bgp group group-name family inet-vpn]
unicast;
```

- To configure an IPv6 IBGP session for Layer 3 VPNs, configure the **unicast** statement at the **[edit protocols bgp group *group-name* family inet6-vpn]** hierarchy level:

```
[edit protocols bgp group group-name family inet6-vpn]
unicast;
```




NOTE: You can configure both `family inet` and `family inet-vpn` or both `family inet6` and `family inet6-vpn` within the same peer group. This allows you to enable support for both IPv4 and IPv4 VPN routes or both IPv6 and IPv6 VPN routes within the same peer group.

Related Documentation

- [Enabling Routing Information Exchange for VPNs on page 19](#)
- [Configuring a Signaling Protocol and LSPs for VPNs on page 22](#)

Configuring Aggregate Labels for VPNs

Aggregate labels for VPNs allow a Juniper Networks routing platform to aggregate a set of incoming labels (labels received from a peer router) into a single forwarding label that is selected from the set of incoming labels. The single forwarding label corresponds to a single next hop for that set of labels. Label aggregation reduces the number of VPN labels that the router must examine.

For a set of labels to share an aggregate forwarding label, they must belong to the same forwarding equivalence class (FEC). The labeled packets must have the same destination egress interface.

Including the `community community-name` statement with the `aggregate-label` statement lets you specify prefixes with a common origin community. Set by policy on the peer PE, these prefixes represent an FEC on the peer PE router.



CAUTION: If the target community is set by mistake instead of the origin community, forwarding problems at the egress PE can result. All prefixes from the peer PE will appear to be in the same FEC, resulting in a single inner label for all CE routers behind a given PE in the same VPN.

To work with route reflectors in Layer 3 VPN networks, the Juniper Networks M10i router aggregates a set of incoming labels only when the routes:

- Are received from the same peer router
- Have the same site of origin community
- Have the same next hop

The next hop requirement is important because route reflectors forward routes originated from different BGP peers to another BGP peer without changing the next hop of those routes.

To configure aggregate labels for VPNs, include the `aggregate-label` statement:

```
aggregate-label {
  community community-name;
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary for this statement.

For information about how to configure a community, see *Understanding BGP Communities and Extended Communities as Routing Policy Match Conditions*.

- Related Documentation**
- *Understanding BGP Communities and Extended Communities as Routing Policy Match Conditions*

Configuring a Signaling Protocol and LSPs for VPNs

For VPNs to function, you must enable a signaling protocol, either the LDP or RSVP on the provider edge (PE) routers and on the provider (P) routers. You also need to configure label-switched paths (LSPs) between the ingress and egress routers. In a typical VPN configuration, you need to configure LSPs from each PE router to all of the other PE routers participating in the VPN in a full mesh.



NOTE: As with any configuration involving MPLS, you cannot configure any of the core-facing interfaces on the PE routers over dense Fast Ethernet PICs.

To enable a signaling protocol, perform the steps in one of the following sections:

- [Using LDP for VPN Signaling on page 22](#)
- [Using RSVP for VPN Signaling on page 24](#)

Using LDP for VPN Signaling

To use LDP for VPN signaling, perform the following steps on the PE and provider (P) routers:

1. Configure LDP on the interfaces in the core of the service provider's network by including the **ldp** statement at the **[edit protocols]** hierarchy level.

You need to configure LDP only on the interfaces between PE routers or between PE and P routers. You can think of these as the “core-facing” interfaces. You do not need to configure LDP on the interface between the PE and customer edge (CE) routers.

```
[edit]
protocols {
  ldp {
    interface type-fpc/pic/port;
  }
}
```

2. Configure the MPLS address family on the interfaces on which you enabled LDP (the interfaces you configured in Step 1) by including the **family mpls** statement at the **[edit interfaces type-fpc/pic/port unit logical-unit-number]** hierarchy level.

```
[edit]
interfaces {
  type-fpc/pic/port {
```

```

        unit logical-unit-number {
            family mpls;
        }
    }
}

```

3. Configure OSPF or IS-IS on each PE and P router.

You configure these protocols at the master instance of the routing protocol, not within the routing instance used for the VPN.

- To configure OSPF, include the **ospf** statement at the **[edit protocols]** hierarchy level. At a minimum, you must configure a backbone area on at least one of the router's interfaces.

```

[edit]
protocols {
    ospf {
        area 0.0.0.0 {
            interface type-fpc/pic/port;
        }
    }
}

```

- To configure IS-IS, include the **isis** statement at the **[edit protocols]** hierarchy level and configure the loopback interface and International Organization for Standardization (ISO) family at the **[edit interfaces]** hierarchy level. At a minimum, you must enable IS-IS on the router, configure a network entity title (NET) on one of the router's interfaces (preferably the loopback interface, lo0), and configure the ISO family on all interfaces on which you want IS-IS to run. When you enable IS-IS, Level 1 and Level 2 are enabled by default. The following is the minimum IS-IS configuration. In the **address** statement, **address** is the NET.

```

[edit]
interfaces {
    lo0 {
        unit logical-unit-number {
            family iso {
                address address;
            }
        }
    }
    type-fpc/pic/port {
        unit logical-unit-number {
            family iso;
        }
    }
}
protocols {
    isis {
        interface all;
    }
}

```

For more information about configuring OSPF and IS-IS, see the *OSPF Feature Guide for Routing Devices* and *IS-IS Feature Guide for Routing Devices*.

Using RSVP for VPN Signaling

To use RSVP for VPN signaling, perform the following steps:

1. On each PE router, configure traffic engineering.

To do this, you must configure an interior gateway protocol (IGP) that supports traffic engineering (either IS-IS or OSPF) and enable traffic engineering support for that protocol.

To enable OSPF traffic engineering support, include the **traffic-engineering** statement at the **[edit protocols ospf]** hierarchy level:

```
[edit protocols ospf]
traffic-engineering {
  shortcuts;
}
```

For IS-IS, traffic engineering support is enabled by default.

2. On each PE and P router, enable RSVP on the interfaces that participate in the label-switched path (LSP).

On the PE router, these interfaces are the ingress and egress points to the LSP. On the P router, these interfaces connect the LSP between the PE routers. Do not enable RSVP on the interface between the PE and the CE routers, because this interface is not part of the LSP.

To configure RSVP on the PE and P routers, include the **interface** statement at the **[edit protocols rsvp]** hierarchy level. Include one **interface** statement for each interface on which you are enabling RSVP.

```
[edit protocols]
rsvp {
  interface interface-name;
  interface interface-name;
}
```

3. On each PE router, configure an MPLS LSP to the PE router that is the LSP's egress point.

To do this, include the **interface** and **label-switched-path** statements at the **[edit protocols mpls]** hierarchy level:

```
[edit protocols]
mpls {
  interface interface-name;
  label-switched-path path-name {
    to ip-address;
  }
}
```

In the **to** statement, specify the address of the LSP's egress point, which is an address on the remote PE router.

In the **interface** statement, specify the name of the interface (both the physical and logical portions). Include one **interface** statement for the interface associated with the LSP.

When you configure the logical portion of the same interface at the **[edit interfaces]** hierarchy level, you must also configure the **family inet** and **family mpls** statements:

```
[edit interfaces]
interface-name {
  unit logical-unit-number {
    family inet;
    family mpls;
  }
}
```

4. On all P routers that participate in the LSP, enable MPLS by including the **interface** statement at the **[edit mpls]** hierarchy level.

Include one **interface** statement for each connection to the LSP.

```
[edit]
mpls {
  interface interface-name;
  interface interface-name;
}
```

5. Enable MPLS on the interface between the PE and CE routers by including the **interface** statement at the **[edit mpls]** hierarchy level.

Doing this allows the PE router to assign an MPLS label to traffic entering the LSP or to remove the label from traffic exiting the LSP.

```
[edit]
mpls {
  interface interface-name;
}
```

For information about configuring MPLS, see the *Minimum MPLS Configuration*.

Related Documentation

- [Minimum MPLS Configuration](#)

Configuring Policies for the VRF Table on PE Routers in VPNs

On each PE router, you must define policies that define how routes are imported into and exported from the router's VRF table. In these policies, you must define the route target, and you can optionally define the route origin.

To configure policy for the VRF tables, you perform the steps in the following sections:

- [Configuring the Route Target on page 26](#)
- [Configuring the Route Origin on page 26](#)
- [Configuring an Import Policy for the PE Router's VRF Table on page 27](#)
- [Configuring an Export Policy for the PE Router's VRF Table on page 29](#)

- [Applying Both the VRF Export and the BGP Export Policies on page 30](#)
- [Configuring a VRF Target on page 31](#)

Configuring the Route Target

As part of the policy configuration for the VPN routing table, you must define a route target, which defines which VPN the route is a part of. When you configure different types of VPN services (Layer 2 VPNs, Layer 3 VPNs, EVPNs, or VPLS) on the same PE router, be sure to assign unique route target values to avoid the possibility of adding route and signaling information to the wrong VPN routing table.

To configure the route target, include the **target** option in the **community** statement:

```
community name members target:community-id;
```

You can include this statement at the following hierarchy levels:

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

name is the name of the community.

community-id is the identifier of the community. Specify it in one of the following formats:

- ***as-number:number***, where *as-number* is an AS number (a 2-byte value) and *number* is a 4-byte community value. The AS number can be in the range 1 through 65,535. We recommend that you use an IANA-assigned, nonprivate AS number, preferably the ISP's own or the customer's own AS number. The community value can be a number in the range 0 through 4,294,967,295 ($2^{32} - 1$).
- ***ip-address:number***, where *ip-address* is an IPv4 address (a 4-byte value) and *number* is a 2-byte community value. The IP address can be any globally unique unicast address. We recommend that you use the address that you configure in the **router-id** statement, which is a nonprivate address in your assigned prefix range. The community value can be a number in the range 1 through 65,535.

Configuring the Route Origin

In the import and export policies for the PE router's VRF table, you can optionally assign the route origin (also known as the site of origin) for a PE router's VRF routes using a VRF export policy applied to multiprotocol external BGP (MP-EBGP) VPN IPv4 route updates sent to other PE routers.

Matching on the assigned route origin attribute in a receiving PE's VRF import policy helps ensure that VPN-IPv4 routes learned through MP-EBGP updates from one PE are not reimported to the same VPN site from a different PE connected to the same site.

To configure a route origin, complete the following steps:

1. Include the **community** statement with the **origin** option:

```
community name members origin:community-id;
```

You can include this statement at the following hierarchy levels:

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

name is the name of the community.

community-id is the identifier of the community. Specify it in one of the following formats:

- ***as-number:number***, where *as-number* is an AS number (a 2-byte value) and *number* is a 4-byte community value. The AS number can be in the range 1 through 65,535. We recommend that you use an IANA-assigned, nonprivate AS number, preferably the ISP's own or the customer's own AS number. The community value can be a number in the range 0 through 4,294,967,295 ($2^{32} - 1$).
 - ***ip-address:number***, where *ip-address* is an IPv4 address (a 4-byte value) and *number* is a 2-byte community value. The IP address can be any globally unique unicast address. We recommend that you use the address that you configure in the **router-id** statement, which is a nonprivate address in your assigned prefix range. The community value can be a number in the range 1 through 65,535.
2. Include the community in the import policy for the PE router's VRF table by configuring the **community** statement with the *community-id* identifier defined in Step 1 at the **[edit policy-options policy-statement *import-policy-name* term *import-term-name* from]** hierarchy level. See [“Configuring an Import Policy for the PE Router's VRF Table” on page 27](#).

If the policy's **from** clause does not specify a community condition, the **vrf-import** statement in which the policy is applied cannot be committed. The Junos OS commit operation does not pass the validation check.
 3. Include the community in the export policy for the PE router's VRF table by configuring the **community** statement with the *community-id* identifier defined in Step 1 at the **[edit policy-options policy-statement *export-policy-name* term *export-term-name* then]** hierarchy level. See [“Configuring an Export Policy for the PE Router's VRF Table” on page 29](#).

See [“Configuring the Route Origin for VPNs” on page 32](#) for a configuration example.

Configuring an Import Policy for the PE Router's VRF Table

Each VPN can have a policy that defines how routes are imported into the PE router's VRF table. An import policy is applied to routes received from other PE routers in the VPN. A policy must evaluate all routes received over the IBGP session with the peer PE router. If the routes match the conditions, the route is installed in the PE router's ***routing-instance-name.inet.0*** VRF table. An import policy must contain a second term that rejects all other routes.

Unless an import policy contains only a **then reject** statement, it must include a reference to a community. Otherwise, when you try to commit the configuration, the commit fails. You can configure multiple import policies.

An import policy determines what to import to a specified VRF table based on the VPN routes learned from the remote PE routers through IBGP. The IBGP session is configured at the **[edit protocols bgp]** hierarchy level. If you also configure an import policy at the **[edit protocols bgp]** hierarchy level, the import policies at the **[edit policy-options]** hierarchy level and the **[edit protocols bgp]** hierarchy level are combined through a logical AND operation. This allows you to filter traffic as a group.

To configure an import policy for the PE router's VRF table, follow these steps:

1. To define an import policy, include the **policy-statement** statement. For all PE routers, an import policy must always include the **policy-statement** statement, at a minimum:

```
policy-statement import-policy-name {  
  term import-term-name {  
    from {  
      protocol bgp;  
      community community-id;  
    }  
    then accept;  
  }  
  term term-name {  
    then reject;  
  }  
}
```

You can include the **policy-statement** statement at the following hierarchy levels:

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

The ***import-policy-name*** policy evaluates all routes received over the IBGP session with the other PE router. If the routes match the conditions in the **from** statement, the route is installed in the PE router's *routing-instance-name*.inet.0 VRF table. The second term in the policy rejects all other routes.

For more information about creating policies, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*.

2. You can optionally use a regular expression to define a set of communities to be used for the VRF import policy.

For example you could configure the following using the **community** statement at the **[edit policy-options policy-statement *policy-statement-name*]** hierarchy level:

```
[edit policy-options vrf-import-policy-sample]  
community high-priority members *:50
```

Note that you cannot configure a regular expression as a part of a route target extended community. For more information about how to configure regular expressions for communities, see *Understanding How to Define BGP Communities and Extended Communities*.

3. To configure an import policy, include the **vrf-import** statement:

```
vrf-import import-policy-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 an Export Policy for the PE Router's VRF Table

Each VPN can have a policy that defines how routes are exported from the PE router's VRF table. An export policy is applied to routes sent to other PE routers in the VPN. An export policy must evaluate all routes received over the routing protocol session with the CE router. (This session can use the BGP, OSPF, or Routing Information Protocol [RIP] routing protocols, or static routes.) If the routes match the conditions, the specified community target (which is the route target) is added to them and they are exported to the remote PE routers. An export policy must contain a second term that rejects all other routes.

Export policies defined within the VPN routing instance are the only export policies that apply to the VRF table. Any export policy that you define on the IBGP session between the PE routers has no effect on the VRF table. You can configure multiple export policies.

To configure an export policy for the PE router's VRF table, follow these steps:

1. For all PE routers, an export policy must distribute VPN routes to and from the connected CE routers in accordance with the type of routing protocol that you configure between the CE and PE routers within the routing instance.

To define an export policy, include the **policy-statement** statement. An export policy must always include the **policy-statement** statement, at a minimum:

```
policy-statement export-policy-name {
  term export-term-name {
    from protocol (bgp | ospf | rip | static);
    then {
      community add community-id;
      accept;
    }
  }
  term term-name {
    then reject;
  }
}
```



NOTE: Configuring the **community add** statement is a requirement for Layer 2 VPN VRF export policies. If you change the **community add** statement to the **community set** statement, the router at the egress of the Layer 2 VPN link might drop the connection.



NOTE: When configuring draft-rosen multicast VPNs operating in source-specific mode and using the `vrf-export` statement to specify the export policy, the policy must have a term that accepts routes from the `vrf-name.mdt.0` routing table. This term ensures proper PE autodiscovery using the `inet-mdt` address family.

When configuring draft-rosen multicast VPNs operating in source-specific mode and using the `vrf-target` statement, the VRF export policy is automatically generated and automatically accepts routes from the `vrf-name.mdt.0` routing table.

You can include the **policy-statement** statement at the following hierarchy levels:

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

The ***export-policy-name*** policy evaluates all routes received over the routing protocol session with the CE router. (This session can use the BGP, OSPF, or RIP routing protocols, or static routes.) If the routes match the conditions in the **from** statement, the community target specified in the **then community add** statement is added to them and they are exported to the remote PE routers. The second term in the policy rejects all other routes.

For more information about creating policies, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*.

2. To apply the policy, include the **vrf-export** statement:

```
vrf-export export-policy-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*]**

Applying Both the VRF Export and the BGP Export Policies

When you apply a VRF export policy as described in “[Configuring an Export Policy for the PE Router's VRF Table](#)” on page 29, routes from VPN routing instances are advertised to other PE routers based on this policy, whereas the BGP export policy is ignored.

If you include the **vpn-apply-export** statement in the BGP configuration, both the VRF export and BGP group or neighbor export policies are applied (VRF first, then BGP) before routes are advertised in the VPN routing tables to other PE routers.

When you include the **vpn-apply-export** statement, be aware of the following:

- Routes imported into the `l3vpn.bgp.0` routing table retain the attributes of the original routes (for example, an OSPF route remains an OSPF route even when it is stored in the `l3vpn.bgp.0` routing table). You should be aware of this when you configure an

export policy for connections between an IBGP PE router and a PE router, a route reflector and a PE router, or AS boundary router (ASBR) peer routers.

- By default, all routes in the l3vpn.bgp.0 routing table are exported to the IBGP peers. If the last statement of the export policy is deny all and if the export policy does not specifically match on routes in the l3vpn.bgp.0 routing table, no routes are exported.

To apply both the VRF export and BGP export policies to VPN routes, include the **vpn-apply-export** statement:

```
vpn-apply-export;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring a VRF Target

Including the **vrf-target** statement in the configuration for a VRF target community causes default VRF import and export policies to be generated that accept and tag routes with the specified target community. You can still create more complex policies by explicitly configuring VRF import and export policies. These policies override the default policies generated when you configure the **vrf-target** statement.

If you do not configure the **import** and **export** options of the **vrf-target** statement, the specified community string is applied in both directions. The **import** and **export** keywords give you more flexibility, allowing you to specify a different community for each direction.

The syntax for the VRF target community is not a name. You must specify it in the format **target:x:y**. A community name cannot be specified because this would also require you to configure the community members for that community using the **policy-options** statement. If you define the **policy-options** statements, then you can just configure VRF import and export policies as usual. The purpose of the **vrf-target** statement is to simplify the configuration by allowing you to configure most statements at the **[edit routing-instances]** hierarchy level.

To configure a VRF target, include the **vrf-target** statement:

```
vrf-target community;
```

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*]**

An example of how you might configure the **vrf-target** statement follows:

```
[edit routing-instances sample]
vrf-target target:69:102;
```

To configure the **vrf-target** statement with the **export** and **import** options, include the following statements:

```
vrf-target {
  export community-name;
```

```
import community-name;
}
```

You can include this statement at the following hierarchy levels:

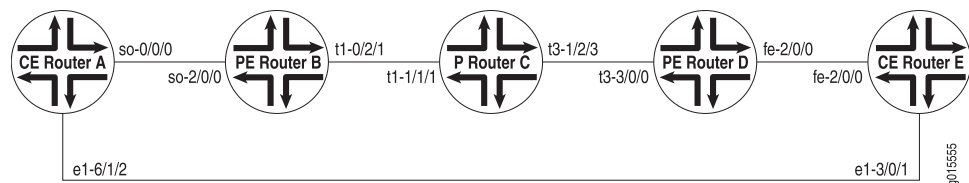
- [edit routing-instances *routing-instance-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*]

Configuring the Route Origin for VPNs

You can use route origin to prevent routes learned from one customer edge (CE) router marked with origin community from being advertised back to it from another CE router in the same AS.

In the example, the route origin is used to prevent routes learned from CE Router A that are marked with origin community from being advertised back to CE Router E by AS 200. The example topology is shown in [Figure 3 on page 32](#).

Figure 3: Network Topology of Site of Origin Example



In this topology, CE Router A and CE Router E are in the same AS (AS200). They use EBGP to exchange routes with their respective provider edge (PE) routers, PE Router B and PE Router D. The two CE routers have a back connection.

The following sections describe how to configure the route origin for a group of VPNs:

- [Configuring the Site of Origin Community on CE Router A on page 32](#)
- [Configuring the Community on CE Router A on page 33](#)
- [Applying the Policy Statement on CE Router A on page 33](#)
- [Configuring the Policy on PE Router D on page 34](#)
- [Configuring the Community on PE Router D on page 34](#)
- [Applying the Policy on PE Router D on page 34](#)

Configuring the Site of Origin Community on CE Router A

The following section describes how to configure CE Router A to advertise routes with a site of origin community to PE Router B for this example.



NOTE: In this example, direct routes are configured to be advertised, but any route can be configured.

Configure a policy to advertise routes with **my-soo** community on CE Router A as follows:

```
[edit]
policy-options {
  policy-statement export-to-my-isp {
    term a {
      from {
        protocol direct;
      }
      then {
        community add my-soo;
        accept;
      }
    }
  }
}
```

Configuring the Community on CE Router A

Configure the **my-soo** community on CE Router A as follows:

```
[edit]
policy-options {
  community my-soo {
    members origin:100:1;
  }
}
```

Applying the Policy Statement on CE Router A

Apply the **export-to-my-isp** policy statement as an export policy to the EBGp peering on the CE Router A as follows:

```
[edit]
protocols {
  bgp {
    group my_isp {
      export export-to-my-isp;
    }
  }
}
```

When you issue the **show route receive-protocol bgp detail** command, you should see the following routes originated from PE Router B with **my-soo** community:

```
user@host> show route receive-protocol bgp 10.12.99.2 detail
inet.0: 16 destinations, 16 routes (15 active, 0 holddown, 1 hidden)
inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
vpn_blue.inet.0: 8 destinations, 10 routes (8 active, 0 holddown, 0 hidden)
* 10.12.33.0/30 (2 entries, 1 announced)
  Nexthop: 10.12.99.2
  AS path: 100 I
  Communities: origin:100:1
10.12.99.0/30 (2 entries, 1 announced)
  Nexthop: 10.12.99.2
  AS path: 100 I
  Communities: origin:100:1
* 10.255.71.177/32 (1 entry, 1 announced)
  Nexthop: 10.12.99.2
  AS path: 100 I
```

```
Communities: origin:100:1
* 192.168.64.0/21 (1 entry, 1 announced)
  Nexthop: 10.12.99.2
  AS path: 100 I
  Communities: origin:100:1
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
mpls.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
bgp.l3vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
__juniper_private1__.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0
hidden)
```

Configuring the Policy on PE Router D

Configure a policy on PE Router D that prevents routes with **my-soo** community tagged by CE Router A from being advertised to CE Router E as follows:

```
[edit]
policy-options {
  policy-statement soo-ce1-policy {
    term a {
      from {
        community my-soo;
      }
      then {
        reject;
      }
    }
  }
}
```

Configuring the Community on PE Router D

Configure the community on PE Router D as follows:

```
[edit]
policy-options {
  community my-soo {
    members origin:100:1;
  }
}
```

Applying the Policy on PE Router D

To prevent routes learned from CE Router A from being advertised to CE Router E (the two routers can communicate these routes directly), apply the **soo-ce1-policy** policy statement as an export policy to the PE Router D and CE Router E EBGP session **vpn_blue**.

View the EBGP session on PE Router D using the **show routing-instances** command.

```
user@host# show routing-instances
vpn_blue {
  instance-type vrf;
  interface fe-2/0/0.0;
  vrf-target target:100:200;
  protocols {
    bgp {
      group ce2 {
```

```
        advertise-peer-as;  
        peer-as 100;  
        neighbor 10.12.99.6;  
    }  
}  
}
```

Apply the **soo-ce1-policy** policy statement as an export policy to the PE Router D and CE Router E EBGP session **vpn_blue** as follows:

```
[edit routing-instances]  
vpn_blue {  
  protocols {  
    bgp {  
      group ce2 {  
        export soo-ce1-policy;  
      }  
    }  
  }  
}
```


CHAPTER 4

Distributing VPN Routes with Target Filtering

- [Configuring BGP Route Target Filtering for VPNs on page 37](#)
- [Example: BGP Route Target Filtering for VPNs on page 39](#)
- [Example: Configuring BGP Route Target Filtering for VPNs on page 41](#)
- [Configuring Static Route Target Filtering for VPNs on page 49](#)
- [Understanding Proxy BGP Route Target Filtering for VPNs on page 50](#)
- [Example: Configuring Proxy BGP Route Target Filtering for VPNs on page 51](#)
- [Example: Configuring an Export Policy for BGP Route Target Filtering for VPNs on page 66](#)
- [Reducing Network Resource Use with Static Route Target Filtering for VPNs on page 82](#)

Configuring BGP Route Target Filtering for VPNs

BGP route target filtering allows you to distribute VPN routes to only the routers that need them. In VPN networks without BGP route target filtering configured, BGP distributes all VPN routes to all VPN peer routers.

For more information about BGP route target filtering, see RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*.

The following sections provide an overview of BGP route target filtering and how to configure it for VPNs:

- [BGP Route Target Filtering Overview on page 37](#)
- [Configuring BGP Route Target Filtering for VPNs on page 38](#)

BGP Route Target Filtering Overview

PE routers, unless they are configured as route reflectors or are running an EBGp session, discard any VPN routes that do not include a route target extended community as specified in the local VRF import policies. This is the default behavior of the Junos OS.

However, unless it is explicitly configured not to store VPN routes, any router configured either as a route reflector or border router for a VPN address family must store all of the

VPN routes that exist in the service provider's network. Also, though PE routers can automatically discard routes that do not include a route target extended community, route updates continue to be generated and received.

By reducing the number of routers receiving VPN routes and route updates, BGP route target filtering helps to limit the amount of overhead associated with running a VPN. BGP route target filtering is most effective at reducing VPN-related administrative traffic in networks where there are many route reflectors or AS border routers that do not participate in the VPNs directly (not acting as PE routers for the CE devices).

BGP route target filtering uses standard UPDATE messages to distribute route target extended communities between routers. The use of UPDATE messages allows BGP to use its standard loop detection mechanisms, path selection, policy support, and database exchange implementation.

Configuring BGP Route Target Filtering for VPNs

BGP route target filtering is enabled through the exchange of the **route-target** address family, stored in the `bgp.rtarget.0` routing table. Based on the **route-target** address family, the route target NLRI (address family indicator [AFI]=1, subsequent AFI [SAFI]=132) is negotiated with its peers.

On a system that has locally configured VRF instances, BGP automatically generates local routes corresponding to targets referenced in the **vrf-import** policies.

To configure BGP route target filtering, include the **family route-target** statement:

```
family route-target {  
    advertise-default;  
    external-paths number;  
    prefix-limit number;  
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

The **advertise-default**, **external-paths**, and **prefix-limit** statements affect the BGP route target filtering configuration as follows:

- The **advertise-default** statement causes the router to advertise the default route target route (0:0:0/0) and suppress all routes that are more specific. This can be used by a route reflector on BGP groups consisting of neighbors that act as PE routers only. PE routers often need to advertise all routes to the route reflector.

Suppressing all route target advertisements other than the default route reduces the amount of information exchanged between the route reflector and the PE routers. The Junos OS further helps to reduce route target advertisement overhead by not maintaining dependency information unless a nondefault route is received.

- The **external-paths** statement (which has a default value of 1) causes the router to advertise the VPN routes that reference a given route target. The number you specify determines the number of external peer routers (currently advertising that route target) that receive the VPN routes.

- The **prefix-limit** statement limits the number of prefixes that can be received from a peer router.

The **route-target**, **advertise-default**, and **external-path** statements affect the RIB-OUT state and must be consistent between peer routers that share the same BGP group. The **prefix-limit** statement affects the receive side only and can have different settings between different peer routers in a BGP group.

Related Documentation

- [Example: Configuring Proxy BGP Route Target Filtering](#)
- [Example: Configuring an Export Policy for BGP Route Target Filtering for VPNs on page 66](#)
- [Example: Configuring BGP Route Target Filtering for VPNs on page 41](#)
- [Configuring the Route Origin for VPNs on page 32](#)
- [Configuring Static Route Target Filtering for VPNs on page 49](#)

Example: BGP Route Target Filtering for VPNs

BGP route target filtering is enabled by configuring the **family route-target** statement at the appropriate BGP hierarchy level. This statement enables the exchange of a new **route-target** address family, which is stored in the `bgp.target.0` routing table.

The following configuration illustrates how you could configure BGP route target filtering for a BGP group titled **to_vpn04**:

```
[edit]
protocols {
  bgp {
    group to_vpn04 {
      type internal;
      local-address 10.255.14.182;
      peer-as 200;
      neighbor 10.255.14.174 {
        family inet-vpn {
          unicast;
        }
        family route-target;
      }
    }
  }
}
```

The following configuration illustrates how you could configure a couple of local VPN routing and forwarding (VRF) routing instances to take advantage of the functionality provided by BGP route target filtering. Based on this configuration, BGP would automatically generate local routes corresponding to the route targets referenced in the VRF import policies (note the targets defined by the **vrf-target** statements).

```
[edit]
routing-instances {
  vpn1 {
```

```

instance-type vrf;
interface t1-0/1/2.0;
vrf-target target:200:101;
protocols {
    ospf {
        export bgp-routes;
        area 0.0.0.0 {
            interface t1-0/1/2.0;
        }
    }
}
}
vpn2 {
    instance-type vrf;
    interface t1-0/1/2.1;
    vrf-target target:200:102;
    protocols {
        ospf {
            export bgp-routes;
            area 0.0.0.0 {
                interface t1-0/1/2.1;
            }
        }
    }
}
}

```

Issue the **show route table bgp.rtarget.0** show command to verify the BGP route target filtering configuration:

```

user@host> show route table bgp.rtarget.0
bgp.rtarget.0: 4 destinations, 6 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
200:200:101/96
    *[RTarget/5] 00:10:00
        Local
200:200:102/96
    *[RTarget/5] 00:10:00
        Local
200:200:103/96
    *[BGP/170] 00:09:48, localpref 100, from 10.255.14.174
        AS path: I
        > t3-0/0/0.0
200:200:104/96
    *[BGP/170] 00:09:48, localpref 100, from 10.255.14.174
        AS path: I
        > t3-0/0/0.0

```

The **show** command display format for route target prefixes is:

AS number:route target extended community/length

The first number represents the autonomous system (AS) of the router that sent this advertisement. The remainder of the display follows the Junos **show** command convention for extended communities.

The output from the **show route table bgp-rtarget.0** command displays the locally generated and remotely generated routes.

The first two entries correspond to the route targets configured for the two local VRF routing instances (**vpn1** and **vpn2**):

- **200:200:101/96**—Community **200:101** in the **vpn1** routing instance
- **200:200:102/96**—Community **200:102** in the **vpn2** routing instance

The last two entries are prefixes received from a BGP peer:

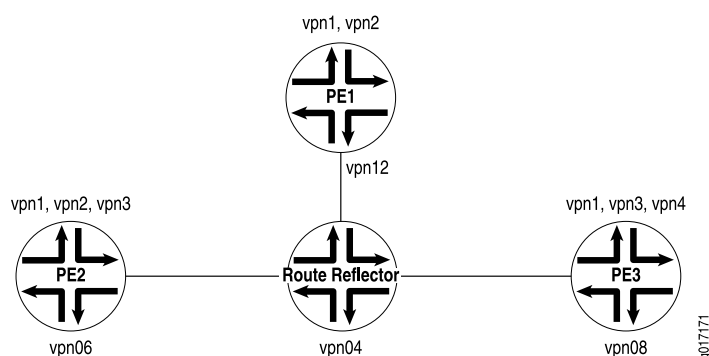
- **200:200:103/96**—Tells the local router that routes tagged with this community (**200:103**) should be advertised to peer **10.255.14.174** through **t3-0/0/0.0**
- **200:200:104/96**—Tells the local router that routes tagged with this community (**200:104**) should be advertised to peer **10.255.14.174** through **t3-0/0/0.0**

Example: Configuring BGP Route Target Filtering for VPNs

BGP route target filtering reduces the number of routers that receive VPN routes and route updates, helping to limit the amount of overhead associated with running a VPN. BGP route target filtering is most effective at reducing VPN-related administrative traffic in networks where there are many route reflectors or AS border routers that do not participate in the VPNs directly (do not act as PE routers for the CE devices).

Figure 4 on page 41 illustrates the topology for a network configured with BGP route target filtering for a group of VPNs.

Figure 4: BGP Route Target Filtering Enabled for a Group of VPNs



The following sections describe how to configure BGP route target filtering for a group of VPNs:

- [Configure BGP Route Target Filtering on Router PE1 on page 41](#)
- [Configure BGP Route Target Filtering on Router PE2 on page 43](#)
- [Configure BGP Route Target Filtering on the Route Reflector on page 45](#)
- [Configure BGP Route Target Filtering on Router PE3 on page 47](#)

Configure BGP Route Target Filtering on Router PE1

This section describes how to enable BGP route target filtering on Router PE1 for this example.

Configure the routing options on router PE1 as follows:

```
[edit]
routing-options {
  route-distinguisher-id 10.255.14.182;
  autonomous-system 200;
}
```

Configure the BGP protocol on Router PE1 as follows:

```
[edit]
protocols {
  bgp {
    group to_VPN_D {
      type internal;
      local-address 10.255.14.182;
      peer-as 200;
      neighbor 10.255.14.174 {
        family inet-vpn {
          unicast;
        }
        family route-target;
      }
    }
  }
}
```

Configure the **vpn1** routing instance as follows:

```
[edit]
routing-instances {
  vpn1 {
    instance-type vrf;
    interface t1-0/1/2.0;
    vrf-target target:200:101;
    protocols {
      ospf {
        export bgp-routes;
        area 0.0.0.0 {
          interface t1-0/1/2.0;
        }
      }
    }
  }
}
```

Configure the **vpn2** routing instance on Router PE1 as follows:

```
[edit]
routing-instances {
  vpn2 {
    instance-type vrf;
    interface t1-0/1/2.1;
    vrf-target target:200:102;
    protocols {
      ospf {
        export bgp-routes;
      }
    }
  }
}
```

```

        area 0.0.0.0 {
            interface t1-0/1/2.1;
        }
    }
}

```

Once you have implemented this configuration, you should see the following when you issue a **show route table bgp.rtarget.0** command:

```

user@host> show route table bgp.rtarget.0
bgp.rtarget.0: 4 destinations, 6 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

200:200:101/96
    *[RTarget/5] 00:27:42
        Local
        [BGP/170] 00:27:30, localpref 100, from
10.255.14.174
        AS path: I
        > via t3-0/0/0.0
200:200:102/96
    *[RTarget/5] 00:27:42
        Local
        [BGP/170] 00:27:30, localpref 100, from
10.255.14.174
        AS path: I
        > via t3-0/0/0.0
200:200:103/96
    *[BGP/170] 00:27:30, localpref 100, from
10.255.14.174
        AS path: I
        > via t3-0/0/0.0
200:200:104/96
    *[BGP/170] 00:27:30, localpref 100, from
10.255.14.174
        AS path: I
        > via t3-0/0/0.0

```

Configure BGP Route Target Filtering on Router PE2

This section describes how to enable BGP route target filtering on Router PE2 for this example.

Configure the routing options on Router PE2 as follows:

```

[edit]
routing-options {
    route-distinguisher-id 10.255.14.176;
    autonomous-system 200;
}

```

Configure the BGP protocol on Router PE2 as follows:

```

[edit]
protocols {
    bgp {
        group to_vpn04 {

```

```
    type internal;
    local-address 10.255.14.176;
    peer-as 200;
    neighbor 10.255.14.174 {
        family inet-vpn {
            unicast;
        }
        family route-target;
    }
}
}
```

Configure the **vpn1** routing instance on Router PE2 as follows:

```
[edit]
routing-instances {
  vpn1 {
    instance-type vrf;
    interface t3-0/0/0.0;
    vrf-target target:200:101;
    protocols {
      bgp {
        group vpn1 {
          type external;
          peer-as 101;
          as-override;
          neighbor 10.49.11.2;
        }
      }
    }
  }
}
```

Configure the **vpn2** routing instance on Router PE2 as follows:

```
[edit]
routing-instances {
  vpn2 {
    instance-type vrf;
    interface t3-0/0/0.1;
    vrf-target target:200:102;
    protocols {
      bgp {
        group vpn2 {
          type external;
          peer-as 102;
          as-override;
          neighbor 10.49.21.2;
        }
      }
    }
  }
}
```

Configure the **vpn3** routing instance on Router PE2 as follows:


```
[edit]
routing-instances {
  vpn3 {
    instance-type vrf;
    interface t3-0/0/0.2;
    vrf-import vpn3-import;
    vrf-export vpn3-export;
    protocols {
      bgp {
        group vpn3 {
          type external;
          peer-as 103;
          as-override;
          neighbor 10.49.31.2;
        }
      }
    }
  }
}
```

Once you have configured router PE2 in this manner, you should see the following when you issue the **show route table bgp.rtarget.0** command:

```
user@host> show route table bgp.rtarget.0
bgp.rtarget.0: 4 destinations, 7 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

200:200:101/96
    *[RTarget/5] 00:28:15
        Local
        [BGP/170] 00:28:03, localpref 100, from
10.255.14.174
    AS path: I
    > via t1-0/1/0.0
200:200:102/96
    *[RTarget/5] 00:28:15
        Local
        [BGP/170] 00:28:03, localpref 100, from
10.255.14.174
    AS path: I
    > via t1-0/1/0.0
200:200:103/96
    *[RTarget/5] 00:28:15
        Local
        [BGP/170] 00:28:03, localpref 100, from
10.255.14.174
    AS path: I
    > via t1-0/1/0.0
200:200:104/96
    *[BGP/170] 00:28:03, localpref 100, from
10.255.14.174
    AS path: I
    > via t1-0/1/0.0
```

Configure BGP Route Target Filtering on the Route Reflector

This section illustrates how to enable BGP route target filtering on the route reflector for this example.

Configure the routing options on the route reflector as follows:

```
[edit]
routing-options {
  route-distinguisher-id 10.255.14.174;
  autonomous-system 200;
}
```

Configure the BGP protocol on the route reflector as follows:

```
[edit]
protocols {
  bgp {
    group rr-group {
      type internal;
      local-address 10.255.14.174;
      cluster 10.255.14.174;
      peer-as 200;
      neighbor 10.255.14.182 {
        description to_PE1_vpn12;
        family inet-vpn {
          unicast;
        }
        family route-target;
      }
      neighbor 10.255.14.176 {
        description to_PE2_vpn06;
        family inet-vpn {
          unicast;
        }
        family route-target;
      }
      neighbor 10.255.14.178 {
        description to_PE3_vpn08;
        family inet-vpn {
          unicast;
        }
        family route-target;
      }
    }
  }
}
```

Once you have configured the route reflector in this manner, you should see the following when you issue the **show route table bgp.rtarget.0** command:

```
user@host> show route table bgp.rtarget.0
bgp.rtarget.0: 4 destinations, 8 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

200:200:101/96
10.255.14.176
    AS path: I
    > via t1-0/2/0.0
    [BGP/170] 00:29:03, localpref 100, from
10.255.14.178
    AS path: I
```

```

10.255.14.182      > via t3-0/1/1.0
                  [BGP/170] 00:29:03, localpref 100, from
                  AS path: I
200:200:102/96    > via t3-0/1/3.0
                  *[BGP/170] 00:29:03, localpref 100, from
10.255.14.176    AS path: I
                  > via t1-0/2/0.0
                  [BGP/170] 00:29:03, localpref 100, from
10.255.14.182    AS path: I
                  > via t3-0/1/3.0
200:200:103/96   *[BGP/170] 00:29:03, localpref 100, from
10.255.14.176    AS path: I
                  > via t1-0/2/0.0
                  [BGP/170] 00:29:03, localpref 100, from
10.255.14.178    AS path: I
                  > via t3-0/1/1.0
200:200:104/96   *[BGP/170] 00:29:03, localpref 100, from
10.255.14.178    AS path: I
                  > via t3-0/1/1.0

```

Configure BGP Route Target Filtering on Router PE3

The following section describes how to enable BGP route target filtering on Router PE3 for this example.

Configure the routing options on Router PE3 as follows:

```

[edit]
routing-options {
  route-distinguisher-id 10.255.14.178;
  autonomous-system 200;
}

```

Configure the BGP protocol on Router PE3 as follows:

```

[edit]
protocols {
  bgp {
    group to_vpn04 {
      type internal;
      local-address 10.255.14.178;
      peer-as 200;
      neighbor 10.255.14.174 {
        family inet-vpn {
          unicast;
        }
        family route-target;
      }
    }
  }
}

```

```
}  
}
```

Configure the **vpn1** routing instance on Router PE3 as follows:

```
[edit]  
routing-instances {  
  vpn1 {  
    instance-type vrf;  
    interface t3-0/0/0.0;  
    vrf-target target:200:101;  
    protocols {  
      rip {  
        group vpn1 {  
          export bgp-routes;  
          neighbor t3-0/0/0.0;  
        }  
      }  
    }  
  }  
}
```

Configure the **vpn3** routing instance on Router PE3 as follows:

```
[edit]  
routing-instances {  
  vpn3 {  
    instance-type vrf;  
    interface t3-0/0/0.1;  
    vrf-target target:200:103;  
    protocols {  
      rip {  
        group vpn3 {  
          export bgp-routes;  
          neighbor t3-0/0/0.1;  
        }  
      }  
    }  
  }  
}
```

Configure the **vpn4** routing instance on Router PE3 as follows:

```
[edit]  
routing-instances {  
  vpn4 {  
    instance-type vrf;  
    interface t3-0/0/0.2;  
    vrf-target target:200:104;  
    protocols {  
      rip {  
        group vpn4 {  
          export bgp-routes;  
          neighbor t3-0/0/0.2;  
        }  
      }  
    }  
  }  
}
```

```

    }
}

```

Once you have configured Router PE3 in this manner, you should see the following when you issue the **show route table bgp.rtarget.0** command:

```

user@host> show route table bgp.rtarget.0
bgp.rtarget.0: 4 destinations, 7 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

200:200:101/96
    *[RTarget/5] 00:29:42
        Local
        [BGP/170] 00:29:30, localpref 100, from
10.255.14.174
    AS path: I
    > via t3-0/0/1.0
200:200:102/96
    *[BGP/170] 00:29:29, localpref 100, from
10.255.14.174
    AS path: I
    > via t3-0/0/1.0
200:200:103/96
    *[RTarget/5] 00:29:42
        Local
        [BGP/170] 00:29:30, localpref 100, from
10.255.14.174
    AS path: I
    > via t3-0/0/1.0
200:200:104/96
    *[RTarget/5] 00:29:42
        Local
        [BGP/170] 00:29:30, localpref 100, from
10.255.14.174
    AS path: I
    > via t3-0/0/1.0

```

Configuring Static Route Target Filtering for VPNs

The BGP VPN route target extended community (RFC 4360, *BGP Extended Communities Attribute*) is used to determine VPN membership. Static route target filtering helps to prevent resources from being consumed in portions of the network where the VPN routes are not needed due to the lack of member PE routers (RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*). Routers can originate routes into the RT-Constrain protocol to indicate their interest in receiving VPN routes containing route targets that match the RT-Constrain NLRI.

To configure static route target filtering for VPNs:

- Configure the **route-target-filter** statement at the **[edit routing-options rib bgp.rtarget.0 static]** hierarchy level.

The following example illustrates how you could configure the **route-target-filter** statement:

```

[edit routing-options rib bgp.rtarget.0 static]
route-target-filter destination {

```

```
group bgp-group;  
local;  
neighbor bgp-peer;  
}
```

- You can display route target filtering information using the **show bgp group rtf detail** command.

**Related
Documentation**

- [Reducing Network Resource Use with Static Route Target Filtering for VPNs on page 82](#)
- [Configuring BGP Route Target Filtering for VPNs on page 37](#)

Understanding Proxy BGP Route Target Filtering for VPNs

BGP route target filtering (also known as route target constrain, or RTC) allows you to distribute VPN routes to only the devices that need them. In VPN networks without BGP route target filtering configured, BGP distributes all VPN routes to all VPN peer devices, which can strain network resources. The route target filtering feature was introduced to reduce the number of devices receiving VPN routes and VPN routing updates, thereby limiting the amount of overhead associated with running a VPN. The Junos OS implementation for BGP route target filtering is based on RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*.

What if you have a network environment where route target filtering is not widely deployed, or what if some devices do not support route target filtering? For example, you might have a BGP speaker with route target filtering enabled that is peered with a BGP speaker that does not support or have route target filtering configured. In this case, the BGP speaker with route target filtering configured must advertise default route target membership (RT membership) on behalf of its peer. The route target filtering resource savings are unrealized because the device supporting the filtering must now send all VPN routes to the device that does not support the filter. Proxy BGP route target filtering (or Proxy RTC) permits the generation of RT membership for devices that do not support route target filtering. This eases the deployment of route target filtering in networks where it is incompletely deployed or not fully supported.

Proxy BGP route target filtering allows you to distribute proxy RT membership advertisements created from the received BGP VPN routes to other devices in the network that need them. These are known as proxy advertisements because the device creates the RT membership on behalf of its peers without the route target filtering functionality. Proxy BGP route target filtering uses BGP route target extended communities that are exported to a specific BGP speaker to generate the route targets. Generated proxy RTC routes are stored in the `bgp.rtarget.0` routing table.

You can also configure a policy to control which VPN routes are used to generate the proxy RTC routes. This can help control which RT membership is generated by the proxying device. In addition, you can configure a policy to reduce the memory overhead associated with proxy RTC. Proxy RTC only uses additional memory on a per-VPN route basis when it is permitted by a policy to be used for generating RT membership.

- Related Documentation**
- [Configuring BGP Route Target Filtering for VPNs on page 37](#)
 - [Example: Configuring Proxy BGP Route Target Filtering for VPNs on page 51](#)
 - [Example: Configuring an Export Policy for BGP Route Target Filtering for VPNs on page 66](#)

Example: Configuring Proxy BGP Route Target Filtering for VPNs

This example shows how to configure proxy BGP route target filtering (also known as proxy route target constrain, or proxy RTC).

- [Requirements on page 51](#)
- [Overview on page 51](#)
- [Configuration on page 53](#)
- [Verification on page 65](#)

Requirements

This example uses the following hardware and software components:

- Four Juniper Networks devices that can be a combination of M Series, MX Series, or T Series routers.
- Junos OS Release 12.2 or later on one or more devices configured for proxy BGP route filtering. In this example, you explicitly configure proxy BGP route filtering on the route reflectors.

Before configuring proxy BGP route target filtering, make sure that you are familiar with and understand the following concepts:

- [Layer 2 VPNs on page 121](#)
- *Layer 3 VPNs*
- *Route distinguishers*
- [Route targets on page 25](#)
- [BGP route target filtering on page 37](#)
- *BGP extended communities*

Overview

Route target filtering decreases the number of devices in a network that receive VPN routes that are not needed. Proxy BGP route target filtering allows networks to take advantage of route target filtering in locations where the feature is not currently supported. By configuring this feature, you can realize many of the same network resource savings that are available to you if your network fully supported BGP route target filtering.

To configure proxy BGP route target filtering, you include the **family route-target proxy-generate** statement on the devices that will distribute proxy route target

membership (RT membership) advertisements for the devices that do not support BGP route target filtering. The proxy BGP route target filtering routes are then stored in the `bgp.rtarget.0` routing table.

Proxy BGP route target filtering is intended to create RT membership advertisements for devices that do not support the BGP route target filtering feature. If the **proxy-generate** statement is present, but the route target family is negotiated with the BGP peer, the proxy-generate functionality is disabled. This allows simplified configuration of BGP peer groups where a portion of the peers in the group support route target filtering but others do not. In such an example case, the **family route-target proxy-generate** statement might be part of the BGP peer group configuration.

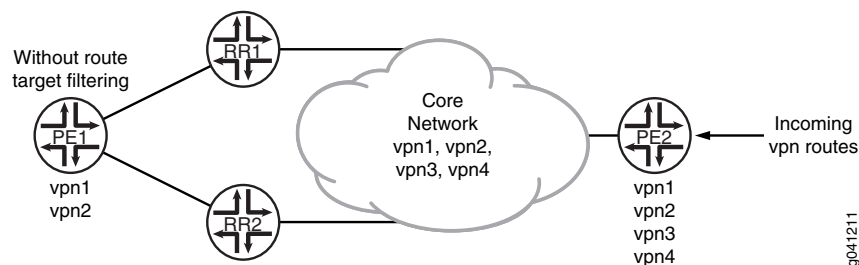


NOTE: When deploying proxy BGP route target filtering in your network, the **advertise-default** statement for BGP route target filtering causes the device to advertise the default route target route (0:0:0/0) and suppress all routes that are more specific. If you have proxy BGP route target filtering configured on one device and one or more peers have the **advertise-default** statement configured as part of their BGP route target filtering configuration, the **advertise-default** configuration is ignored.

Topology Diagram

Figure 5 on page 52 shows the topology used in this example.

Figure 5: Proxy BGP Route Target Filtering Topology



In this example, BGP route target filtering is configured on the route reflectors (Device RR1 and Device RR2) and the provider edge (PE) Device PE2, but the other PE, Device PE1, does not support the BGP route target filtering functionality. Device PE2 has four VPNs configured (vpn1, vpn2, vpn3, and vpn4). Device PE1 has two VPNs configured (vpn1 and vpn2), so this device is only interested in receiving route updates for vpn1 and vpn2. Currently, this is impossible because both route reflectors (Device RR1 and Device RR2) learn and share information about all of the incoming VPN routes (vpn1 through vpn4) with Device PE1. In the sample topology, all devices participate in autonomous system (AS) 200, OSPF is the configured interior gateway protocol (IGP), and LDP is the signaling protocol used by the VPNs. In this example, we use static routes in the VPN routing and forwarding (VRF) instances to generate VPN routes. This is done in place of using a PE to customer edge (CE) protocol such as OSPF or BGP.

To minimize the number of VPN route updates being processed by Device PE1, you include the **family route-target proxy-generate** statement to configure proxy BGP route target filtering on each route reflector. Each route reflector has a peering session with Device PE1 and supports route target filtering to the core. However, Device PE1 does not support route target filtering, so the network resource savings are unrealized by Device PE1 since it receives all of the VPN updates. By configuring proxy BGP route target filtering on the peering sessions facing Device PE1, you limit the number of VPN updates processed by Device PE1, and the route reflectors generate the proxy BGP route target routes for Device PE1 throughout the network.

Configuration

- [Configuring Device PE1 on page 55](#)
- [Configuring Device RR1 on page 57](#)
- [Configuring Device RR2 on page 60](#)
- [Configuring Device PE2 on page 62](#)

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 PE1	<pre> set interfaces ge-1/0/0 unit 0 description PE1-to-RR1 set interfaces ge-1/0/0 unit 0 family inet address 10.49.0.1/30 set interfaces ge-1/0/0 unit 0 family mpls set interfaces ge-1/0/1 unit 0 description PE1-to-RR2 set interfaces ge-1/0/1 unit 0 family inet address 10.49.10.1/30 set interfaces ge-1/0/1 unit 0 family mpls set protocols ldp interface ge-1/0/0 set protocols ldp interface ge-1/0/1 set protocols bgp group internal type internal set protocols bgp group internal local-address 10.255.163.58 set protocols bgp group internal neighbor 10.255.165.220 family inet-vpn unicast set protocols bgp group internal neighbor 10.255.165.28 family inet-vpn unicast set protocols ospf area 0.0.0.0 interface ge-1/0/0 set protocols ospf area 0.0.0.0 interface ge-1/0/1 set protocols ospf area 0.0.0.0 interface lo0.0 passive set routing-options route-distinguisher-id 10.255.163.58 set routing-options autonomous-system 200 set routing-instances vpn1 instance-type vrf set routing-instances vpn1 vrf-target target:200:100 set routing-instances vpn1 routing-options static route 203.0.113.1/24 discard set routing-instances vpn2 instance-type vrf set routing-instances vpn2 vrf-target target:200:101 set routing-instances vpn2 routing-options static route 203.0.113.2/24 discard </pre>
Device RR1	<pre> set interfaces ge-1/0/0 unit 0 description RR1-to-PE1 set interfaces ge-1/0/0 unit 0 family inet address 10.49.0.2/30 set interfaces ge-1/0/0 unit 0 family mpls set interfaces ge-1/0/1 unit 0 description RR1-to-PE2 set interfaces ge-1/0/1 unit 0 family inet address 10.50.0.2/30 set interfaces ge-1/0/1 unit 0 family mpls set protocols ldp interface ge-1/0/0 </pre>

```
set protocols ldp interface ge-1/0/1
set protocols bgp group internal type internal
set protocols bgp group internal local-address 110.255.165.220
set protocols bgp group internal cluster 192.0.2.1
set protocols bgp group internal neighbor 10.255.163.58 description vpn1-to-pe1 family
    inet-vpn unicast
set protocols bgp group internal neighbor 10.255.163.58 family route-target proxy-generate
set protocols bgp group internal neighbor 10.255.168.42 description vpn1-to-pe2 family
    inet-vpn unicast
set protocols bgp group internal neighbor 10.255.168.42 family route-target
set protocols ospf area 0.0.0.0 interface ge-1/0/0
set protocols ospf area 0.0.0.0 interface ge-1/0/1
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set routing-options route-distinguisher-id 10.255.165.220
set routing-options autonomous-system 200
```

Device RR2

```
set interfaces ge-1/0/0 unit 0 description RR2-to-PE1
set interfaces ge-1/0/0 unit 0 family inet address 10.49.10.2/30
set interfaces ge-1/0/0 unit 0 family mpls
set interfaces ge-1/0/1 unit 0 description RR2-to-PE2
set interfaces ge-1/0/1 unit 0 family inet address 10.50.10.2/30
set interfaces ge-1/0/1 unit 0 family mpls
set protocols ldp interface ge-1/0/0
set protocols ldp interface ge-1/0/1
set protocols bgp group internal type internal
set protocols bgp group internal local-address 10.255.165.28
set protocols bgp group internal cluster 192.0.2.1
set protocols bgp group internal neighbor 10.255.163.58 description vpn2-to-pe1 family
    inet-vpn unicast
set protocols bgp group internal neighbor 10.255.163.58 family route-target proxy-generate
set protocols bgp group internal neighbor 10.255.168.42 description vpn2-to-pe2 family
    inet-vpn unicast
set protocols bgp group internal neighbor 10.255.168.42 family route-target
set protocols ospf area 0.0.0.0 interface ge-1/0/0
set protocols ospf area 0.0.0.0 interface ge-1/0/1
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set routing-options route-distinguisher-id 10.255.165.28
set routing-options autonomous-system 200
```

Device PE2

```
set interfaces ge-1/0/0 unit 0 description PE2-to-RR1
set interfaces ge-1/0/0 unit 0 family inet address 10.50.0.1/30
set interfaces ge-1/0/0 unit 0 family mpls
set interfaces ge-1/0/1 unit 0 description PE2-to-RR2
set interfaces ge-1/0/1 unit 0 family inet address 10.50.10.1/30
set interfaces ge-1/0/1 unit 0 family mpls
set protocols ldp interface ge-1/0/0
set protocols ldp interface ge-1/0/1
set protocols bgp group internal type internal
set protocols bgp group internal local-address 10.255.168.42
set protocols bgp group internal family inet-vpn unicast
set protocols bgp group internal family route-target
set protocols bgp group internal neighbor 10.255.165.220
set protocols bgp group internal neighbor 10.255.165.28
set protocols ospf area 0.0.0.0 interface ge-1/0/0
set protocols ospf area 0.0.0.0 interface ge-1/0/1
```

```

set protocols ospf area 0.0.0.0 interface lo0.0 passive
set routing-options route-distinguisher-id 10.255.168.42
set routing-options autonomous-system 200
set routing-instances vpn1 instance-type vrf
set routing-instances vpn1 vrf-target target:200:100
set routing-instances vpn1 routing-options static route 203.0.113.1/24 discard
set routing-instances vpn2 instance-type vrf
set routing-instances vpn2 vrf-target target:200:101
set routing-instances vpn2 routing-options static route 203.0.113.2/24 discard
set routing-instances vpn3 instance-type vrf
set routing-instances vpn3 vrf-target target:200:103
set routing-instances vpn3 routing-options static route 203.0.113.3/24 discard
set routing-instances vpn4 instance-type vrf
set routing-instances vpn4 vrf-target target:200:104
set routing-instances vpn4 routing-options static route 203.0.113.4/24 discard

```

Configuring Device PE1

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 Device PE1:

1. Configure the interfaces.

```

[edit interfaces]
user@PE1# set ge-1/0/0 unit 0 description PE1-to-RR1
user@PE1# set ge-1/0/0 unit 0 family inet address 10.49.0.1/30
user@PE1# set ge-1/0/0 unit 0 family mpls

user@PE1# set ge-1/0/1 unit 0 description PE1-to-RR2
user@PE1# set ge-1/0/1 unit 0 family inet address 10.49.10.1/30
user@PE1# set ge-1/0/1 unit 0 family mpls

```

2. Configure the route distinguisher and the AS number.

```

[edit routing-options]
user@PE1# set route-distinguisher-id 10.255.163.58
user@PE1# set autonomous-system 200

```

3. Configure LDP as the signaling protocol used by the VPN.

```

[edit protocols ldp]
user@PE1# set interface ge-1/0/0
user@PE1# set interface ge-1/0/1

```

4. Configure BGP.

```

[edit protocols bgp group internal]
user@PE1# set type internal
user@PE1# set local-address 10.255.163.58
user@PE1# set neighbor 10.255.165.220 family inet-vpn unicast
user@PE1# set neighbor 10.255.165.28 family inet-vpn unicast

```

5. Configure OSPF.

```

[edit protocols ospf area 0.0.0.0]

```

```
user@PE1# set interface ge-1/0/0
user@PE1# set interface ge-1/0/1
user@PE1# set interface lo0.0 passive
```

6. Configure the VPN routing instances.

```
[edit routing-instances vpn1]
user@PE1# set instance-type vrf
user@PE1# set vrf-target target:200:100
user@PE1# set routing-options static route 203.0.113.1/24 discard

[edit routing-instances vpn2]
user@PE1# set instance-type vrf
user@PE1# set vrf-target target:200:101
user@PE1# set routing-options static route 203.0.113.2/24 discard
```

7. If you are done configuring the device, commit the configuration.

```
[edit]
user@PE1# commit
```

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

```
user@PE1# show interfaces
ge-1/0/0 {
  unit 0 {
    description PE1-to-RR1;
    family inet {
      address 10.49.0.1/30;
    }
    family mpls;
  }
}
ge-1/0/1 {
  unit 0 {
    description PE1-to-RR2;
    family inet {
      address 10.49.10.1/30;
    }
    family mpls;
  }
}

user@PE1# show protocols
bgp {
  group internal {
    type internal;
    local-address 10.255.163.58;
    neighbor 10.255.165.220 {
      family inet-vpn {
        unicast;
      }
    }
  }
  neighbor 10.255.165.28 {
```

```

        family inet-vpn {
            unicast;
        }
    }
}
}
ospf {
    area 0.0.0.0 {
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
        interface lo0.0 {
            passive;
        }
    }
}
ldp {
    interface ge-1/0/0.0;
    interface ge-1/0/1.0;
}

user@PE1# show routing-options
route-distinguisher-id 10.255.14.182;
autonomous-system 200;

user@PE1# show routing-instances
vpn1 {
    instance-type vrf;
    vrf-target target:200:100;
    routing-options {
        static {
            route 203.0.113.1/24 discard;
        }
    }
}
vpn2 {
    instance-type vrf;
    vrf-target target:200:101;
    routing-options {
        static {
            route 203.0.113.2/24 discard;
        }
    }
}
}

```

Configuring Device RR1

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 Device RR1:

1. Configure the interfaces.

```

[edit interfaces]
user@RR1# set ge-1/0/0 unit 0 description RR1-to-PE1
user@RR1# set ge-1/0/0 unit 0 family inet address 10.49.0.2/30

```

```
user@RR1# set ge-1/0/0 unit 0 family mpls
```

```
user@RR1# set ge-1/0/1 unit 0 description RR1-to-PE2
user@RR1# set ge-1/0/1 unit 0 family inet address 10.50.0.2/30
user@RR1# set ge-1/0/1 unit 0 family mpls
```

2. Configure the route distinguisher and the AS number.

```
[edit routing-options]
user@RR1# set route-distinguisher-id 10.255.165.220
user@RR1# set autonomous-system 200
```

3. Configure LDP as the signaling protocol used by the VPN.

```
[edit protocols ldp]
user@RR1# set interface ge-1/0/0
user@RR1# set interface ge-1/0/1
```

4. Configure BGP.

```
[edit protocols bgp group internal]
user@RR1# set type internal
user@RR1# set local-address 10.255.165.220
user@RR1# set cluster 192.0.2.1
user@RR1# set neighbor 10.255.163.58 description vpn1-to-pe1 family inet-vpn
unicast
user@RR1# set neighbor 10.255.168.42 description vpn1-to-pe2 family inet-vpn
unicast
```

5. Configure BGP route target filtering on the peering session with Device PE2.

```
[edit protocols bgp group internal]
user@RR1# set neighbor 10.255.168.42 family route-target
```

6. Configure proxy BGP route target filtering on the peering session with Device PE1.

```
[edit protocols bgp group internal]
user@RR1# set neighbor 10.255.163.58 family route-target proxy-generate
```

7. Configure OSPF.

```
[edit protocols ospf area 0.0.0.0]
user@RR1# set interface ge-1/0/0
user@RR1# set interface ge-1/0/1
user@RR1# set interface lo0.0 passive
```

8. If you are done configuring the device, commit the configuration.

```
[edit]
user@RR1# commit
```

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

```
user@RR1# show interfaces
ge-1/0/0 {
  unit 0 {
    description RR1-to-PE1;
    family inet {
```

```

        address 10.49.0.2/30;
    }
    family mpls;
}
}
ge-1/0/1 {
    unit 0 {
        description RR1-to-PE2;
        family inet {
            address 10.50.0.2/30;
        }
        family mpls;
    }
}

user@RR1# show protocols
bgp {
    group internal {
        type internal;
        local-address 110.255.165.220;
        cluster 192.0.2.1;
        neighbor 10.255.163.58 {
            description vpn1-to-pe1;
            family inet-vpn {
                unicast;
            }
            family route-target {
                proxy-generate;
            }
        }
        neighbor 10.255.168.42 {
            description vpn1-to-pe2;
            family inet-vpn {
                unicast;
            }
            family route-target;
        }
    }
}

ospf {
    area 0.0.0.0 {
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
        interface lo0.0 {
            passive;
        }
    }
}

ldp {
    interface ge-1/0/0.0;
    interface ge-1/0/1.0;
}

user@RR1# show routing-options
route-distinguisher-id 10.255.165.220;
autonomous-system 200;

```

Configuring Device RR2

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 Device RR2:

1. Configure the interfaces.

```
[edit interfaces]
user@RR2# set ge-1/0/0 unit 0 description RR2-to-PE1
user@RR2# set ge-1/0/0 unit 0 family inet address 10.49.10.2/30
user@RR2# set ge-1/0/0 unit 0 family mpls

user@RR2# set ge-1/0/1 unit 0 description RR2-to-PE2
user@RR2# set ge-1/0/1 unit 0 family inet address 10.50.10.2/30
user@RR2# set ge-1/0/1 unit 0 family mpls
```
2. Configure the route distinguisher and the AS number.

```
[edit routing-options]
user@RR2# set route-distinguisher-id 10.255.165.28
user@RR2# set autonomous-system 200
```
3. Configure LDP as the signaling protocol used by the VPN.

```
[edit protocols ldp]
user@RR2# set interface ge-1/0/0
user@RR2# set interface ge-1/0/1
```
4. Configure BGP.

```
[edit protocols bgp group internal]
user@RR2# set type internal
user@RR2# set local-address 10.255.165.28
user@RR2# set cluster 192.0.2.1
user@RR2# set neighbor 10.255.163.58 description vpn2-to-pe1 family inet-vpn
unicast
user@RR2# set neighbor 10.255.168.42 description vpn2-to-pe2 family inet-vpn
unicast
```
5. Configure BGP route target filtering on the peering session with Device PE2.

```
[edit protocols bgp group internal]
user@RR2# set neighbor 10.255.168.42 family route-target
```
6. Configure proxy BGP route target filtering on the peering session with Device PE1.

```
[edit protocols bgp group internal]
user@RR2# set neighbor 10.255.163.58 family route-target proxy-generate
```
7. Configure OSPF.

```
[edit protocols ospf area 0.0.0.0]
user@RR2# set interface ge-1/0/0
user@RR2# set interface ge-1/0/1
user@RR2# set interface lo0.0 passive
```
8. If you are done configuring the device, commit the configuration.


```
[edit]
user@RR2# commit
```

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

```
user@RR2# show interfaces
ge-1/0/0 {
  unit 0 {
    description RR2-to-PE1;
    family inet {
      address 10.49.10.2/30;
    }
    family mpls;
  }
}
ge-1/0/1 {
  unit 0 {
    description RR2-to-PE2;
    family inet {
      address 10.50.10.2/30;
    }
    family mpls;
  }
}

user@RR2# show protocols
bgp {
  group internal {
    local-address 10.255.165.28;
    cluster 192.0.2.1;
    neighbor 10.255.163.58 {
      description vpn2-to-pe1;
      family inet-vpn {
        unicast;
      }
      family route-target {
        proxy-generate;
      }
    }
    neighbor 10.255.168.42 {
      description vpn2-to-pe2;
      family inet-vpn {
        unicast;
      }
      family route-target;
    }
  }
}
ospf {
  area 0.0.0.0 {
    interface ge-1/0/0.0;
    interface ge-1/0/1.0;
    interface lo0.0 {
```

```

        passive;
    }
}
}
ldp {
    interface ge-1/0/0.0;
    interface ge-1/0/1.0;
}

user@RR2# show routing-options
route-distinguisher-id 10.255.165.28;
autonomous-system 200;

```

Configuring Device PE2

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 Device PE2:

1. Configure the interfaces.

```

[edit interfaces]
user@PE2# set ge-1/0/0 unit 0 description PE2-to-RR1
user@PE2# set ge-1/0/0 unit 0 family inet address 10.50.0.1/30
user@PE2# set ge-1/0/0 unit 0 family mpls

user@PE2# set ge-1/0/1 unit 0 description PE2-to-RR2
user@PE2# set ge-1/0/1 unit 0 family inet address 10.50.10.1/30
user@PE2# set ge-1/0/1 unit 0 family mpls

```

2. Configure the route distinguisher and the AS number.

```

[edit routing-options]
user@PE2# set route-distinguisher-id 10.255.168.42
user@PE2# set autonomous-system 200

```

3. Configure LDP as the signaling protocol used by the VPN.

```

[edit protocols ldp]
user@PE2# set interface ge-1/0/0
user@PE2# set interface ge-1/0/1

```

4. Configure BGP.

```

[edit protocols bgp group internal]
user@PE2# set type internal
user@PE2# set local-address 10.255.168.42
user@PE2# set family inet-vpn unicast
user@PE2# set family route-target
user@PE2# set neighbor 10.255.165.220
user@PE2# set neighbor 10.255.165.28

```

5. Configure OSPF.

```

[edit protocols ospf area 0.0.0.0]
user@PE2# set interface ge-1/0/0
user@PE2# set interface ge-1/0/1

```

```
user@PE2# set interface lo0.0 passive
```

6. Configure the VPN routing instances.

```
[edit routing-instances vpn1]
user@PE2# set instance-type vrf
user@PE2# set vrf-target target:200:100
user@PE2# set routing-options static route 203.0.113.1/24 discard
```

```
[edit routing-instances vpn2]
user@PE2# set instance-type vrf
user@PE2# set vrf-target target:200:101
user@PE2# set routing-options static route 203.0.113.2/24 discard
```

```
[edit routing-instances vpn3]
user@PE2# set instance-type vrf
user@PE2# set vrf-target target:200:103
user@PE2# set routing-options static route 203.0.113.3/24 discard
```

```
[edit routing-instances vpn4]
user@PE2# set instance-type vrf
user@PE2# set vrf-target target:200:104
user@PE2# set routing-options static route 203.0.113.4/24 discard
```

7. If you are done configuring the device, commit the configuration.

```
[edit]
user@PE2# commit
```

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

```
user@PE2# show interfaces
ge-1/0/0 {
  unit 0 {
    description PE2-to-RR1;
    family inet {
      address 10.50.0.1/30;
    }
    family mpls;
  }
}
ge-1/0/1 {
  unit 0 {
    description PE2-to-RR2;
    family inet {
      address 10.50.10.1/30;
    }
    family mpls;
  }
}

user@PE2# show protocols
bgp {
  group internal {
    type internal;
```

```
        local-address 10.255.168.42;
        family inet-vpn {
            unicast;
        }
        family route-target;
        neighbor 10.255.165.220;
        neighbor 10.255.165.28;
    }
}
ospf {
    area 0.0.0.0 {
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
        interface lo0.0 {
            passive;
        }
    }
}
ldp {
    interface ge-1/0/0.0;
    interface ge-1/0/1.0;
}

user@PE2# show routing-options
route-distinguisher-id 10.255.168.42;
autonomous-system 200;

user@PE2# show routing-instances
vpn1 {
    instance-type vrf;
    vrf-target target:200:100;
    routing-options {
        static {
            route 203.0.113.1/24 discard;
        }
    }
}
vpn2 {
    instance-type vrf;
    vrf-target target:200:101;
    routing-options {
        static {
            route 203.0.113.2/24 discard;
        }
    }
}
vpn3 {
    instance-type vrf;
    vrf-target target:200:103;
    routing-options {
        static {
            route 203.0.113.3/24 discard;
        }
    }
}
vpn4 {
    instance-type vrf;
```

```

vrf-target target:200:104;
routing-options {
  static {
    route 203.0.113.4/24 discard;
  }
}
}

```

Verification

Confirm that the configuration is working properly.

Verifying the Proxy BGP Route Target Routes

Purpose Verify that the proxy BGP route target routes are displayed in the `bgp.rtarget.0` table on Device RR1.

Action From operational mode, enter the `show route table bgp.rtarget.0` command to display the proxy BGP route targets.

```

user@RR1# show route table bgp.rtarget.0
4 destinations, 6 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

200:200:100/96
    * [RTarget/5] 00:01:22
      Type Proxy
      for 10.255.163.58
      Local
      [BGP/170] 00:04:55, localpref 100, from 10.255.168.42
      AS path: I, validation-state: unverified
      > to 10.50.0.1 via ge-1/0/1

200:200:101/96
    * [RTarget/5] 00:01:22
      Type Proxy
      for 10.255.163.58
      Local
      [BGP/170] 00:04:55, localpref 100, from 10.255.168.42
      AS path: I, validation-state: unverified
      > to 10.50.0.1 via ge-1/0/1

200:200:103/96
    * [BGP/170] 00:04:55, localpref 100, from 10.255.168.42
      AS path: I, validation-state: unverified
      > to 10.50.0.1 via ge-1/0/1

200:200:104/96
    * [BGP/170] 00:04:55, localpref 100, from 10.255.168.42
      AS path: I, validation-state: unverified
      > to 10.50.0.1 via ge-1/0/1

```

Meaning Device RR1 is generating the proxy BGP route target routes on behalf of its peer Device PE1. The proxy BGP route target routes are identified with the protocol and preference `[RTarget/5]` and the route target type of `Proxy`.

Related Documentation

- [Example: Configuring an Export Policy for BGP Route Target Filtering for VPNs on page 66](#)

- [Configuring BGP Route Target Filtering for VPNs on page 37](#)
- [Understanding Proxy BGP Route Target Filtering for VPNs on page 50](#)

Example: Configuring an Export Policy for BGP Route Target Filtering for VPNs

This example shows how to configure an export routing policy for BGP route target filtering (also known as route target constrain, or RTC).

- [Requirements on page 66](#)
- [Overview on page 66](#)
- [Configuration on page 68](#)
- [Verification on page 81](#)

Requirements

This example uses the following hardware and software components:

- Four Juniper Networks devices that support BGP route target filtering.
- Junos OS Release 12.2 or later on one or more devices configured for proxy BGP route filtering. In this example, you explicitly configure proxy BGP route filtering on the route reflectors.

Before configuring an export policy for BGP route target filtering, make sure that you are familiar with and understand the following concepts:

- [Layer 2 VPNs on page 121](#)
- *Layer 3 VPNs*
- *Route distinguishers*
- [Route targets on page 25](#)
- [BGP route target filtering on page 37](#)
- *BGP extended communities*

Overview

BGP route target filtering allows you to reduce network resource consumption by distributing route target membership (RT membership) advertisements throughout the network. BGP uses the RT membership information to send VPN routes only to the devices that need them in the network. Similar to other types of BGP reachability, you can apply a routing policy to route target filtering routes to influence the network. When route target filtering is configured, restricting the flow of route target filtering routes also restricts the VPN routes that might be attracted by this RT membership. Configuring this policy involves:

- Creating a filter that defines the list of route target prefixes.

- Creating a policy to select a subset of the route target filters to use for BGP route target filtering.

To define the list of route target prefixes:

- You configure the **rtf-prefix-list** statement at the **[edit policy-options]** hierarchy level to specify the name of the route target prefix list and one or more route target prefixes to use. This configuration allows you to specify the incoming route target filtering routes that the device will use and then distribute them throughout the network.

To configure the routing policy and apply the route target prefix list to that policy, you can specify the following policy options:

- **family route-target**—(Optional) The route-target family match condition specifies matching BGP route target filtering routes. You define this criteria in the **from** statement. This example shows how to create an export policy using the **family route-target** match condition.
- **protocol route-target**—(Optional) The route-target protocol match condition defines the criteria that an incoming route must match. You define this criteria in the **from** statement. This statement is primarily useful for restricting the policy to locally generated route target filtering routes.



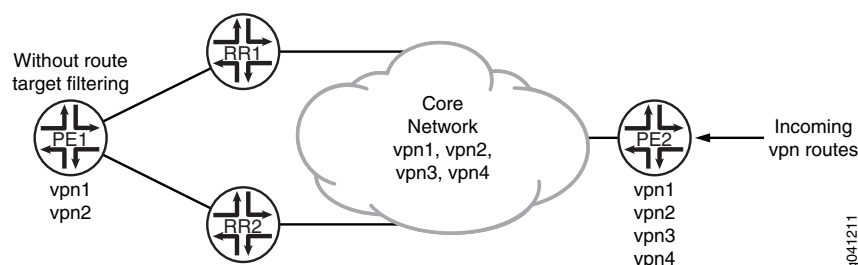
NOTE: When you use the `show route table bgp.rtarget.0` command to view proxy BGP route target filtering routes, you will see the BGP protocol for received routes and the route target protocol routes for local route target filtering routes.

- **rtf-prefix-list name**—The **rtf-prefix-list** statement applies the list of route target prefixes that you already configured to the policy. You define this criteria in the **from** statement.

Topology Diagram

Figure 6 on page 67 shows the topology used in this example.

Figure 6: BGP Route Target Filtering Export Policy Topology



In this example, BGP route target filtering is configured on the route reflectors (Device RR1 and Device RR2) and provider edge (PE) Device PE2. The other PE, Device PE1, does not support BGP route target filtering. Proxy BGP route target filtering is also configured on the peering sessions between the route reflectors and Device PE1 to minimize the number of VPN route updates processed by Device PE1. Device PE2 has four VPNs

configured (vpn1, vpn2, vpn3, and vpn4), and Device PE1 has two VPNs configured (vpn1 and vpn2). In the sample topology, all devices participate in autonomous system (AS) 200, OSPF is the configured interior gateway protocol (IGP), and LDP is the signaling protocol used by the VPNs. In this example, we use static routes in the VPN routing and forwarding (VRF) instances to generate VPN routes. This is done in place of using a PE to customer edge (CE) protocol such as OSPF or BGP.

In this example, you further control the routes being advertised from Device PE2 to Device PE1 by configuring an export policy on Device PE2 to prevent vpn3 routes from being advertised to Device RR1. You create a policy that specifies the **family route-target** match condition, defines the list of route target prefixes, and applies the list of route target prefixes by defining the **rtf-prefix-list** criteria.

Configuration

- [Configuring Device PE1 on page 70](#)
- [Configuring Device RR1 on page 73](#)
- [Configuring Device RR2 on page 75](#)
- [Configuring Device PE2 on page 77](#)

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 PE1	<pre> set interfaces ge-1/0/0 unit 0 description PE1-to-RR1 set interfaces ge-1/0/0 unit 0 family inet address 10.49.0.1/30 set interfaces ge-1/0/0 unit 0 family mpls set interfaces ge-1/0/1 unit 0 description PE1-to-RR2 set interfaces ge-1/0/1 unit 0 family inet address 10.49.10.1/30 set interfaces ge-1/0/1 unit 0 family mpls set protocols ldp interface ge-1/0/0 set protocols ldp interface ge-1/0/1 set protocols bgp group internal type internal set protocols bgp group internal local-address 10.255.163.58 set protocols bgp group internal neighbor 10.255.165.220 family inet-vpn unicast set protocols bgp group internal neighbor 10.255.165.28 family inet-vpn unicast set protocols ospf area 0.0.0.0 interface ge-1/0/0 set protocols ospf area 0.0.0.0 interface ge-1/0/1 set protocols ospf area 0.0.0.0 interface lo0.0 passive set routing-options route-distinguisher-id 10.255.163.58 set routing-options autonomous-system 200 set routing-instances vpn1 instance-type vrf set routing-instances vpn1 vrf-target target:200:100 set routing-instances vpn1 routing-options static route 203.0.113.1/24 discard set routing-instances vpn2 instance-type vrf set routing-instances vpn2 vrf-target target:200:101 set routing-instances vpn2 routing-options static route 203.0.113.2/24 discard </pre>
Device RR1	<pre> set interfaces ge-1/0/0 unit 0 description RR1-to-PE1 set interfaces ge-1/0/0 unit 0 family inet address 10.49.0.2/30 set interfaces ge-1/0/0 unit 0 family mpls set interfaces ge-1/0/1 unit 0 description RR1-to-PE2 </pre>


```

set interfaces ge-1/0/1 unit 0 family inet address 10.50.0.2/30
set interfaces ge-1/0/1 unit 0 family mpls
set protocols ldp interface ge-1/0/0
set protocols ldp interface ge-1/0/1
set protocols bgp group internal type internal
set protocols bgp group internal local-address 10.255.165.220
set protocols bgp group internal cluster 192.0.2.1
set protocols bgp group internal neighbor 10.255.163.58 description vpn1-to-pe1 family
    inet-vpn unicast
set protocols bgp group internal neighbor 10.255.163.58 family route-target proxy-generate
set protocols bgp group internal neighbor 10.255.168.42 description vpn1-to-pe2 family
    inet-vpn unicast
set protocols ospf area 0.0.0.0 interface ge-1/0/0
set protocols ospf area 0.0.0.0 interface ge-1/0/1
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set routing-options route-distinguisher-id 10.255.165.220
set routing-options autonomous-system 200

```

Device RR2

```

set interfaces ge-1/0/0 unit 0 description RR2-to-PE1
set interfaces ge-1/0/0 unit 0 family inet address 10.49.10.2/30
set interfaces ge-1/0/0 unit 0 family mpls
set interfaces ge-1/0/1 unit 0 description RR2-to-PE2
set interfaces ge-1/0/1 unit 0 family inet address 10.50.10.2/30
set interfaces ge-1/0/1 unit 0 family mpls
set protocols ldp interface ge-1/0/0
set protocols ldp interface ge-1/0/1
set protocols bgp group internal type internal
set protocols bgp group internal local-address 10.255.165.28
set protocols bgp group internal cluster 192.0.2.1
set protocols bgp group internal neighbor 10.255.163.58 description vpn2-to-pe1 family
    inet-vpn unicast
set protocols bgp group internal neighbor 10.255.163.58 family route-target proxy-generate
set protocols bgp group internal neighbor 10.255.168.42 description vpn2-to-pe2 family
    inet-vpn unicast
set protocols bgp group internal neighbor 10.255.163.58 family route-target
set protocols ospf area 0.0.0.0 interface ge-1/0/0
set protocols ospf area 0.0.0.0 interface ge-1/0/1
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set routing-options route-distinguisher-id 10.255.165.28
set routing-options autonomous-system 200

```

Device PE2

```

set interfaces ge-1/0/0 unit 0 description PE2-to-RR1
set interfaces ge-1/0/0 unit 0 family inet address 10.50.0.1/30
set interfaces ge-1/0/0 unit 0 family mpls
set interfaces ge-1/0/1 unit 0 description PE2-to-RR2
set interfaces ge-1/0/1 unit 0 family inet address 10.50.10.2/30
set interfaces ge-1/0/1 unit 0 family mpls
set protocols ldp interface ge-1/0/0
set protocols ldp interface ge-1/0/1
set protocols bgp group internal type internal
set protocols bgp group internal local-address 10.255.168.42
set protocols bgp group internal family inet-vpn unicast
set protocols bgp group internal family route-target
set protocols bgp group internal neighbor 10.255.165.220 export filter-rtc
set protocols bgp group internal neighbor 10.255.165.28

```

```

set protocols ospf area 0.0.0.0 interface ge-1/0/0
set protocols ospf area 0.0.0.0 interface ge-1/0/1
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set policy-options rtf-prefix-list exclude-103 200:200:103/96
set policy-options policy-statement filter-rtc from family route-target
set policy-options policy-statement filter-rtc from rtf-prefix-list exclude-103
set policy-options policy-statement filter-rtc then reject
set routing-options route-distinguisher-id 10.255.168.42
set routing-options autonomous-system 200
set routing-instances vpn1 instance-type vrf
set routing-instances vpn1 vrf-target target:200:100
set routing-instances vpn1 routing-options static route 203.0.113.1/24 discard
set routing-instances vpn2 instance-type vrf
set routing-instances vpn2 vrf-target target:200:101
set routing-instances vpn2 routing-options static route 203.0.113.2/24 discard
set routing-instances vpn3 instance-type vrf
set routing-instances vpn3 vrf-target target:200:103
set routing-instances vpn3 routing-options static route 203.0.113.3/24 discard
set routing-instances vpn4 instance-type vrf
set routing-instances vpn4 vrf-target target:200:104
set routing-instances vpn4 routing-options static route 203.0.113.4/24 discard

```

Configuring Device PE1

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 Device PE1:

1. Configure the interfaces.

```

[edit interfaces]
user@PE1# set ge-1/0/0 unit 0 description PE1-to-RR1
user@PE1# set ge-1/0/0 unit 0 family inet address 10.49.0.1/30
user@PE1# set ge-1/0/0 unit 0 family mpls

```

```

user@PE1# set ge-1/0/1 unit 0 description PE1-to-RR2
user@PE1# set ge-1/0/1 unit 0 family inet address 10.49.10.1/30
user@PE1# set ge-1/0/1 unit 0 family mpls

```

2. Configure the route distinguisher and the AS number.

```

[edit routing-options]
user@PE1# set route-distinguisher-id 10.255.163.58
user@PE1# set autonomous-system 200

```

3. Configure LDP as the signaling protocol used by the VPN.

```

[edit protocols ldp]
user@PE1# set interface ge-1/0/0
user@PE1# set interface ge-1/0/1

```

4. Configure BGP.

```

[edit protocols bgp group internal]
user@PE1# set type internal
user@PE1# set local-address 10.255.163.58

```

```

user@PE1# set neighbor 10.255.165.220 family inet-vpn unicast
user@PE1# set neighbor 10.255.165.28 family inet-vpn unicast

```

5. Configure OSPF.

```

[edit protocols ospf area 0.0.0.0]
user@PE1# set interface ge-1/0/0
user@PE1# set interface ge-1/0/1
user@PE1# set interface lo0.0 passive

```

6. Configure the VPN routing instances.

```

[edit routing-instances vpn1]
user@PE1# set instance-type vrf
user@PE1# set vrf-target target:200:100
user@PE1# set routing-options static route 203.0.113.1/24 discard

[edit routing-instances vpn2]
user@PE1# set instance-type vrf
user@PE1# set vrf-target target:200:101
user@PE1# set routing-options static route 203.0.113.2/24 discard

```

7. If you are done configuring the device, commit the configuration.

```

[edit]
user@PE1# commit

```

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

```

user@PE1# show interfaces
ge-1/0/0 {
  unit 0 {
    description PE1-to-RR1;
    family inet {
      address 10.49.0.1/30;
    }
    family mpls;
  }
}
ge-1/0/1 {
  unit 0 {
    description PE1-to-RR2;
    family inet {
      address 10.49.10.1/30;
    }
    family mpls;
  }
}

user@PE1# show protocols
bgp {
  group internal {
    type internal;
    local-address 10.255.163.58;
    neighbor 10.255.165.220 {

```

```
        family inet-vpn {
            unicast;
        }
    }
    neighbor 10.255.165.28 {
        family inet-vpn {
            unicast;
        }
    }
}
ospf {
    area 0.0.0.0 {
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
        interface lo0.0 {
            passive;
        }
    }
}
ldp {
    interface ge-1/0/0.0;
    interface ge-1/0/1.0;
}

user@PE1# show routing-options
route-distinguisher-id 10.255.14.182;
autonomous-system 200;

user@PE1# show routing-instances
vpn1 {
    instance-type vrf;
    vrf-target target:200:100;
    routing-options {
        static {
            route 203.0.113.1/24 discard;
        }
    }
}
vpn2 {
    instance-type vrf;
    vrf-target target:200:101;
    routing-options {
        static {
            route 203.0.113.2/24 discard;
        }
    }
}
```

Configuring Device RR1

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 Device RR1:

1. Configure the interfaces.

```
[edit interfaces]
user@RR1# set ge-1/0/0 unit 0 description RR1-to-PE1
user@RR1# set ge-1/0/0 unit 0 family inet address 10.49.0.2/30
user@RR1# set ge-1/0/0 unit 0 family mpls
user@RR1# set ge-1/0/1 unit 0 description RR1-to-PE2
user@RR1# set ge-1/0/1 unit 0 family inet address 10.50.0.2/30
user@RR1# set ge-1/0/1 unit 0 family mpls
```
2. Configure the route distinguisher and the AS number.

```
[edit routing-options]
user@RR1# set route-distinguisher-id 10.255.165.220
user@RR1# set autonomous-system 200
```
3. Configure LDP as the signaling protocol used by the VPN.

```
[edit protocols ldp]
user@RR1# set interface ge-1/0/0
user@RR1# set interface ge-1/0/1
```
4. Configure BGP.

```
[edit protocols bgp group internal]
user@RR1# set type internal
user@RR1# set local-address 10.255.165.220
user@RR1# set cluster 192.0.2.1
user@RR1# set neighbor 10.255.163.58 description vpn1-to-pe1 family inet-vpn
unicast
user@RR1# set neighbor 10.255.168.42 description vpn1-to-pe2 family inet-vpn
unicast
```
5. Configure BGP route target filtering on the peering session with Device PE2.

```
[edit protocols bgp group internal]
user@RR1# set neighbor 10.255.168.42 family route-target
```
6. Configure proxy BGP route target filtering on the peering session with Device PE1.

```
[edit protocols bgp group internal]
user@RR1# set neighbor 10.255.163.58 family route-target proxy-generate
```
7. Configure OSPF.

```
[edit protocols ospf area 0.0.0.0]
user@RR1# set interface ge-1/0/0
user@RR1# set interface ge-1/0/1
user@RR1# set interface lo0.0 passive
```
8. If you are done configuring the device, commit the configuration.

```
[edit]
```

```
user@RR1# commit
```

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

```
user@RR1# show interfaces
ge-1/0/0 {
  unit 0 {
    description RR1-to-PE1;
    family inet {
      address 10.49.0.2/30;
    }
    family mpls;
  }
}
ge-1/0/1 {
  unit 0 {
    description RR1-to-PE2;
    family inet {
      address 10.50.0.2/30;
    }
    family mpls;
  }
}

user@RR1# show protocols
bgp {
  group internal {
    type internal;
    local-address 110.255.165.220;
    cluster 192.0.2.1;
    neighbor 10.255.163.58 {
      description vpn1-to-pe1;
      family inet-vpn {
        unicast;
      }
      family route-target {
        proxy-generate;
      }
    }
    neighbor 10.255.168.42 {
      description vpn1-to-pe2;
      family inet-vpn {
        unicast;
      }
      family route-target;
    }
  }
}
ospf {
  area 0.0.0.0 {
    interface ge-1/0/0.0;
    interface ge-1/0/1.0;
    interface lo0.0 {
```

```

        passive;
    }
}
}
ldp {
    interface ge-1/0/0.0;
    interface ge-1/0/1.0;
}
ospf {
    area 0.0.0.0 {
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
        interface lo0.0 {
            passive;
        }
    }
}
ldp {
    interface ge-1/0/0.0;
    interface ge-1/0/1.0;
}

user@RR1# show routing-options
route-distinguisher-id 10.255.165.220;
autonomous-system 200;

```

Configuring Device RR2

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 Device RR2:

1. Configure the interfaces.


```

[edit interfaces]
user@RR2# set ge-1/0/0 unit 0 description RR2-to-PE1
user@RR2# set ge-1/0/0 unit 0 family inet address 10.49.10.2/30
user@RR2# set ge-1/0/0 unit 0 family mpls

user@RR2# set ge-1/0/1 unit 0 description RR2-to-PE2
user@RR2# set ge-1/0/1 unit 0 family inet address 10.50.10.2/30
user@RR2# set ge-1/0/1 unit 0 family mpls

```
2. Configure the route distinguisher and the AS number.


```

[edit routing-options]
user@RR2# set route-distinguisher-id 10.255.165.28
user@RR2# set autonomous-system 200

```
3. Configure LDP as the signaling protocol used by the VPN.


```

[edit protocols ldp]
user@RR2# set interface ge-1/0/0
user@RR2# set interface ge-1/0/1

```
4. Configure BGP.

```
[edit protocols bgp group internal]
user@RR2# set type internal
user@RR2# set local-address 10.255.165.28
user@RR2# set cluster 192.0.2.1
user@RR2# set neighbor 10.255.163.58 description vpn2-to-pe1 family inet-vpn
unicast
user@RR2# set neighbor 10.255.168.42 description vpn2-to-pe2 family inet-vpn
unicast
```

5. Configure BGP route target filtering on the peering session with Device PE2.

```
[edit protocols bgp group internal]
user@RR2# set neighbor 10.255.168.42 family route-target
```

6. Configure proxy BGP route target filtering on the peering session with Device PE1.

```
[edit protocols bgp group internal]
user@RR2# set neighbor 10.255.163.58 family route-target proxy-generate
```

7. Configure OSPF.

```
[edit protocols ospf area 0.0.0.0]
user@RR2# set interface ge-1/0/0
user@RR2# set interface ge-1/0/1
user@RR2# set interface lo0.0 passive
```

8. If you are done configuring the device, commit the configuration.

```
[edit]
user@RR2# commit
```

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

```
user@RR2# show interfaces
ge-1/0/0 {
  unit 0 {
    description RR2-to-PE1;
    family inet {
      address 10.49.10.2/30;
    }
    family mpls;
  }
}
ge-1/0/1 {
  unit 0 {
    description RR2-to-PE2;
    family inet {
      address 10.50.10.2/30;
    }
    family mpls;
  }
}

user@RR2# show protocols
bgp {
  group internal {
```



```

local-address 10.255.165.28;
cluster 192.0.2.1;
neighbor 10.255.163.58 {
  description vpn2-to-pe1;
  family inet-vpn {
    unicast;
  }
  family route-target {
    proxy-generate;
  }
}
neighbor 10.255.168.42 {
  description vpn2-to-pe2;
  family inet-vpn {
    unicast;
  }
  family route-target;
}
}
}
ospf {
  area 0.0.0.0 {
    interface ge-1/0/0.0;
    interface ge-1/0/1.0;
    interface lo0.0 {
      passive;
    }
  }
}
}
ldp {
  interface ge-1/0/0.0;
  interface ge-1/0/1.0;
}
}

user@RR2# show routing-options
route-distinguisher-id 10.255.165.28;
autonomous-system 200;

```

Configuring Device PE2

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 Device PE2:

1. Configure the interfaces.

```

[edit interfaces]
user@PE2# set ge-1/0/0 unit 0 description PE2-to-RR1
user@PE2# set ge-1/0/0 unit 0 family inet address 10.50.0.1/30
user@PE2# set ge-1/0/0 unit 0 family mpls

user@PE2# set ge-1/0/1 unit 0 description PE2-to-RR2
user@PE2# set ge-1/0/1 unit 0 family inet address 10.50.10.2/30
user@PE2# set ge-1/0/1 unit 0 family mpls

```

2. Configure the route distinguisher and the AS number.

```
[edit routing-options]  
user@PE2# set route-distinguisher-id 10.255.168.42  
user@PE2# set autonomous-system 200
```
3. Configure LDP as the signaling protocol used by the VPN.

```
[edit protocols ldp]  
user@PE2# set interface ge-1/0/0  
user@PE2# set interface ge-1/0/1
```
4. Configure BGP.

```
[edit protocols bgp group internal]  
user@PE2# set type internal  
user@PE2# set local-address 10.255.168.42  
user@PE2# set family inet-vpn unicast  
user@PE2# set family route-target  
user@PE2# set neighbor 10.255.165.220  
user@PE2# set neighbor 10.255.165.28
```
5. Configure OSPF.

```
[edit protocols ospf area 0.0.0.0]  
user@PE2# set interface ge-1/0/0  
user@PE2# set interface ge-1/0/1  
user@PE2# set interface lo0.0 passive
```
6. Configure the VPN routing instances.

```
[edit routing-instances vpn1]  
user@PE2# set instance-type vrf  
user@PE2# set vrf-target target:200:100  
user@PE2# set routing-options static route 203.0.113.1/24 discard  
  
[edit routing-instances vpn2]  
user@PE2# set instance-type vrf  
user@PE2# set vrf-target target:200:101  
user@PE2# set routing-options static route 203.0.113.2/24 discard  
  
[edit routing-instances vpn3]  
user@PE2# set instance-type vrf  
user@PE2# set vrf-target target:200:103  
user@PE2# set routing-options static route 203.0.113.3/24 discard  
  
[edit routing-instances vpn4]  
user@PE2# set instance-type vrf  
user@PE2# set vrf-target target:200:104  
user@PE2# set routing-options static route 203.0.113.4/24 discard
```
7. Configure and apply the export routing policy.

```
[edit policy-options]  
user@PE2# set rtf-prefix-list exclude-103 200:200:103/96  
  
[edit policy-options policy-statement filter-rtc]  
user@PE2# set from family route-target  
user@PE2# set from rtf-prefix-list exclude-103  
user@PE2# set then reject
```

```
[edit protocols bgp group internal]
user@PE2# set neighbor 10.255.165.220 export filter-rtc
```

8. If you are done configuring the device, commit the configuration.

```
[edit]
user@PE2# commit
```

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

```
user@PE2# show interfaces
ge-1/0/0 {
  unit 0 {
    description PE2-to-RR1;
    family inet {
      address 10.50.0.1/30;
    }
    family mpls;
  }
}
ge-1/0/1 {
  unit 0 {
    description PE2-to-RR2;
    family inet {
      address 10.50.10.2/30;
    }
    family mpls;
  }
}

user@PE2# show protocols
bgp {
  group internal {
    type internal;
    local-address 10.255.168.42;
    family inet-vpn {
      unicast;
    }
    family route-target;
    neighbor 10.255.165.220 {
      export filter-rtc;
    }
    neighbor 10.255.165.28;
  }
}
ospf {
  area 0.0.0.0 {
    interface ge-1/0/0.0;
    interface ge-1/0/1.0;
    interface lo0.0 {
      passive;
    }
  }
}
```

```
}
ldp {
    interface ge-1/0/0.0;
    interface ge-1/0/1.0;
}

user@PE2# show routing-options
route-distinguisher-id 10.255.168.42;
autonomous-system 200;

user@PE2# show policy-options
policy-statement filter-rtc {
    from {
        family route-target;
        rtf-prefix-list exclude-103;
    }
    then reject;
}
rtf-prefix-list exclude-103 {
    200:200:103/96;
}

user@PE2# show routing-instances
vpn1 {
    instance-type vrf;
    vrf-target target:200:100;
    routing-options {
        static {
            route 203.0.113.1/24 discard;
        }
    }
}
vpn2 {
    instance-type vrf;
    vrf-target target:200:101;
    routing-options {
        static {
            route 203.0.113.2/24 discard;
        }
    }
}
vpn3 {
    instance-type vrf;
    vrf-target target:200:103;
    routing-options {
        static {
            route 203.0.113.3/24 discard;
        }
    }
}
vpn4 {
    instance-type vrf;
    vrf-target target:200:104;
    routing-options {
        static {
            route 203.0.113.4/24 discard;
        }
    }
}
```

```

    }
  }

```

Verification

Confirm that the configuration is working properly.

- [Verifying the Route Target Filtering Routes in the bgp.rtarget.0 Routing Table for Device RR1 on page 81](#)
- [Verifying the Route Target Filtering Routes in the bgp.rtarget.0 Routing Table for Device RR2 on page 81](#)

Verifying the Route Target Filtering Routes in the bgp.rtarget.0 Routing Table for Device RR1

Purpose Verify that the route prefix for vpn3 is not in Device RR1's bgp.rtarget.0 table. Since an export policy on Device PE2 was applied to prevent the advertisement of vpn3 routes to Device RR1, Device RR1 should not receive those advertisements.

Action From operational mode, enter the **show route advertising-protocol bgp 10.255.165.220 table bgp.rtarget.0** command.

```

user@PE2# show route advertising-protocol bgp 10.255.165.220 table bgp.rtarget.0
bgp.rtarget.0: 4 destinations, 11 routes
(4 active, 0 holddown, 0 hidden)

```

Prefix	Nexthop	MED	Lc1pref	AS path
200:200:100/96	*	Self	100	I
200:200:101/96	*	Self	100	I
200:200:104/96	*	Self	100	I

Meaning The bgp.rtarget.0 table does not display 200:200:103/96, which is the route prefix for vpn3. That means the export policy was applied correctly.

Verifying the Route Target Filtering Routes in the bgp.rtarget.0 Routing Table for Device RR2

Purpose Verify that the route prefix for vpn3 is in Device RR2's bgp.rtarget.0 table. Since an export policy was not applied on Device PE2 to prevent the advertisement of vpn3 routes to Device RR2, Device RR2 should receive advertisements from all of the VPNs.

Action From operational mode, enter the **show route advertising-protocol bgp 10.255.165.28 table bgp.rtarget.0** command.

```

user@PE2# show route advertising-protocol bgp 10.255.165.28 table bgp.rtarget.0
bgp.rtarget.0: 4 destinations, 11 routes (4 active, 0 holddown, 0 hidden)
(4 active, 0 holddown, 0 hidden)

```

Prefix	Nexthop	MED	Lc1pref	AS path
200:200:100/96	*	Self	100	I
200:200:101/96	*	Self	100	I
200:200:103/96	*	Self	100	I
200:200:104/96	*	Self	100	I

Meaning The bgp.rtarget.0 table displays the route prefixes for all of the VPNs.

- Related Documentation**
- [Example: Configuring Proxy BGP Route Target Filtering](#)
 - [Configuring BGP Route Target Filtering for VPNs on page 37](#)

Reducing Network Resource Use with Static Route Target Filtering for VPNs

The BGP VPN route target extended community (RFC 4360, *BGP Extended Communities Attribute*) is used to determine VPN membership. Static route target filtering helps to prevent resources from being consumed in portions of the network where the VPN routes are not needed due to the lack of member PE routers (RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*). Routers can originate routes into the RT-Constrain protocol to indicate their interest in receiving VPN routes containing route targets that match the RT-Constrain NLRI.

Normally, for the RT-Constrain feature to function properly, it must be broadly deployed throughout a network. If this is not the case, the feature is less useful, because the RT-Constrain BGP speaker facing a non-RT-Constrain speaker must advertise a default RT-Constrain route to the other RT-Constrain speakers on behalf of the peer that does not support the feature. This effectively removes the resource saving benefits of the feature in portions of the network where it is not supported since a default RT-Constrain route causes the PE router and all intervening PE routers to need to receive all VPN routes.

The static RT-Constrain feature enables you to partially deploy the RT-Constrain feature in a network. The feature is enabled at a boundary in the network where RT-Constrain is configured. However, some BGP VPN peers do not support RT-Constrain, typically PE routers. The route targets of those PE routers must be statically configured on the router. These route targets are disseminated using the RT-Constrain protocol.

The proxy RT-Constrain feature permits BGP VPN peers that do not support the protocol to have their route-targets discovered and disseminated automatically. However, this feature can only support symmetric route-targets. For example, the import and export route-targets for a VRF routing instance are identical. However, for a hub-and-spoke VPN, the import and export route-targets are not identical. In this scenario, the import and export route-target may be statically configured to be disseminated in the RT-Constrain protocol.

- Related Documentation**
- [Configuring Static Route Target Filtering for VPNs on page 49](#)
 - [Configuring BGP Route Target Filtering for VPNs on page 37](#)

CHAPTER 5

Configuring Forwarding Options for VPNs

- [Chained Composite Next Hops for Transit Devices for VPNs on page 83](#)
- [Example: Configuring Chained Composite Next Hops for Direct PE-PE Connections in VPNs on page 85](#)

Chained Composite Next Hops for Transit Devices for VPNs

The Juniper Networks PTX Series Packet Transport Routers, MX Series 3D Universal Edge Routers with MIC and MPC interfaces, T4000 Core Routers, and QFX10000 switches are principally designed to handle large volumes of transit traffic in the core of large networks. Chained composite next hops help to facilitate this capability by allowing the router to process much larger volumes of routes. A chained composite next hop allows the router to direct sets of routes sharing the same destination to a common forwarding next hop, rather than having each route also include the destination. In the event that a network destination is changed, rather than having to update all of the routes sharing that destination with the new information, just the shared forwarding next hop is updated with the new information. The chained composite next hops continue to point to this forwarding next hop which now contains the new destination.

When the next hops for MPLS LSPs are created on the routers, the tag information corresponding to the inner-most MPLS label is extracted into a chained composite next hop. The chained composite next hop is stored in the ingress PFE. The chained composite next hop points to a next hop called the forwarding next hop that resides on the egress PFE. The forwarding next hop contains all of the other information (all of the labels except for the inner-most labels; and the IFA/IP information corresponding to the actual next hop node). Many chained composite next hops can share the same forwarding next hop. Additionally, separating the label from the forwarding next hop and storing it on the ingress PFE (within the chained composite next hop) helps to conserve egress PFE memory by reducing the number of rewrite strings stored on the egress PFE.

The support of chained composite next hops for directly connected Provider Edge (PE) routers varies from one platform to another.

On platforms containing only MPCs, such as PTX Series Packet Transport Routers, the MX80 router, the MX2020 router, and the QFX10000 switches, chained composite next hops are enabled by default for the following MPLS and VPN protocols and applications:



NOTE: Point-to-Multipoint LSPs and Layer 2 VPNs are not supported on the QFX10000 switches.

- Labeled BGP
- Layer 2 VPNs
- Layer 3 VPNs
- LDP
- MPLS
- Point-to-Multipoint LSPs
- RSVP
- Static LSPs

On MX Series 3D Universal Edge Routers containing both DPC and MPC FPCs and on T4000 Core Routers containing MPC and FPCs, chained composite next hops are disabled by default and need to be explicitly configured.

To enable chained composite next hops include the **l3vpn** statement at the **[edit routing-options forwarding-table chained-composite-next-hop ingress]** hierarchy level.

Starting with Junos OS Release 13.3, for chained composite next hop feature to take effect for directly connected PE devices, the chassis must be configured to use the **enhanced-ip** option (in the case of MX Series 3D Universal Edge Routers containing both DPC and MPC FPCs) or the **enhanced-mode** option (in the case of T4000 Core Routers containing MPC and FPCs) in the network service mode, in addition to the **l3vpn** configuration.

For more information about configuring chassis network services, see the *Junos OS Administration Library for Routing Devices*.

Related Documentation

- *Accepting Route Updates with Unique Inner VPN Labels in Layer 3 VPNs*
- [Example: Configuring Chained Composite Next Hops for Direct PE-PE Connections in VPNs on page 85](#)
- *transit (Chained Composite Next Hops)*

Example: Configuring Chained Composite Next Hops for Direct PE-PE Connections in VPNs

This example shows how to enable back-to-back Provider Edge (PE) router Layer 3 Virtual Private Network (VPN) connections with chained composite next hops for MIC and MPC interfaces on MX Series and T4000 routers.

- [Requirements on page 85](#)
- [Overview on page 85](#)
- [Configuration on page 86](#)
- [Verification on page 94](#)

Requirements

This example uses the following hardware and software components:

- Six routers that can be a combination of MX240, MX480, MX960, or T4000 routers.
- Junos OS Release 13.3 running on all the devices.

Before you begin:

1. Configure the device interfaces.
2. Configure the following routing protocols on all the routers:
 - a. MPLS
 - b. BGP
 - c. LDP LSPs as tunnels between the PE devices
 - d. OSPF or any other IGP protocol

Overview

Prior to Junos OS Release 13.3, in a degenerated Layer 3 VPN case without the presence of an MPLS core router, previous behavior of flattened out indirect next hop and unicast next hop was utilized because there was no outer label available in the back-to-back PE-PE connection, and the ingress PE only pushed single VPN labels. In a Layer 3 VPN multipath scenario with mixed PE-PE and PE-P-PE paths, chained composite next hops could not be used either.

On platforms that support only MIC and MPC interfaces, chained composite next hops are enabled by default. On platforms that support both DPC and MPC interfaces, the Layer 3 VPN configuration required the **pe-pe-connection** statement to support chained composite next hops for PE-PE connections. However, the **pe-pe-connection** statement was not supported on platforms with MIC and FPC interfaces only.

As a solution to these limitations, starting with Junos OS Release 13.3, the support for chained composite next hops is enhanced to automatically identify the underlying platform capability on composite next hops at startup time, without relying on user

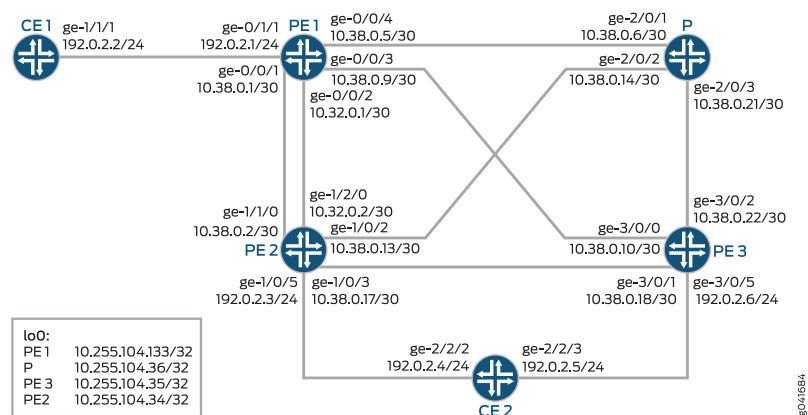
configuration, and to decide the next hop type (composite or indirect) to embed in the Layer 3 VPN label. This enhances the support for back-to-back PE-PE connections in Layer 3 VPN with composite next hops, and eliminates the need for the **pe-pe-connection** statement.

To enable chained composite next hops for directly connected PE devices, in addition to including the **l3vpn** statement at the **[edit routing-options forwarding-table chained-composite-next-hop ingress]** hierarchy level, make the following changes:

- On MX Series 3D Universal Edge Routers containing both DPC and MPC FPCs, chained composite next hops are disabled by default. To enable chained composite next hops on the MX240, MX480, and MX960, the chassis must be configured to use the **enhanced-ip** option in network services mode.
- On T4000 Core Routers containing MPC and FPCs, chained composite next hops are disabled by default. To enable chained composite next hops on a T4000 router, the chassis must be configured to use the **enhanced-mode** option in network services mode.

Topology

Figure 7: Chained Composite Next Hop for PE-PE Connections



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.

```
CE1 set interfaces ge-1/1/1 unit 0 family inet address 192.0.2.2/24
    set interfaces ge-1/1/1 unit 0 family iso
    set interfaces ge-1/1/1 unit 0 family mpls
    set interfaces lo0 unit 0 family inet address 192.0.2.1/24
    set protocols bgp group PE type external
    set protocols bgp group PE peer-as 200
    set protocols bgp group PE neighbor 192.0.2.1
    set routing-options autonomous-system 100
```

```

PE1  set interfaces ge-0/0/1 unit 0 family inet address 10.38.0.1/30
      set interfaces ge-0/0/1 unit 0 family mpls
      set interfaces ge-0/0/2 unit 0 family inet address 10.38.0.5/30
      set interfaces ge-0/0/2 unit 0 family mpls
      set interfaces ge-0/0/3 unit 0 family inet address 10.38.0.9/30
      set interfaces ge-0/0/3 unit 0 family mpls
      set interfaces ge-0/0/4 unit 0 family inet address 10.32.0.1/30
      set interfaces ge-0/0/4 unit 0 family mpls
      set interfaces ge-0/1/1 unit 0 family inet address 192.0.2.1/24
      set interfaces ge-0/1/1 unit 0 family mpls
      set interfaces lo0 unit 0 family inet address 10.255.104.133/32
      set chassis network-services enhanced-ip
      set routing-options forwarding-table chained-composite-next-hop ingress l3vpn
      set routing-options autonomous-system 200
      set routing-options forwarding-table export lbpp
      set protocols mpls interface 10.38.0.1/30
      set protocols mpls interface 10.32.0.1/30
      set protocols mpls interface 10.38.0.5/30
      set protocols mpls interface 10.38.0.9/30
      set protocols bgp group PEs type internal
      set protocols bgp group PEs local-address 10.255.104.133
      set protocols bgp group PEs family inet unicast
      set protocols bgp group PEs family inet-vpn unicast
      set protocols bgp group PEs neighbor 10.255.104.134 local-preference 200
      set protocols bgp group PEs neighbor 10.255.104.135
      set protocols ospf area 0.0.0.0 interface all
      set protocols ospf area 0.0.0.0 interface fxp0.0 disable
      set protocols ospf area 0.0.0.0 interface lo0.0 passive
      set protocols ldp interface all
      set protocols ldp interface fxp0.0 disable
      set policy-options policy-statement lbpp then load-balance per-packet
      set routing-instances vpn-a instance-type vrf
      set routing-instances vpn-a interface ge-0/1/1.0
      set routing-instances vpn-a route-distinguisher 200:1
      set routing-instances vpn-a vrf-target target:200:1
      set routing-instances vpn-a vrf-table-label
      set routing-instances vpn-a protocols bgp group CE type external
      set routing-instances vpn-a protocols bgp group CE peer-as 100
      set routing-instances vpn-a protocols bgp group CE neighbor 192.0.2.2

PE2  set interfaces ge-1/0/2 unit 0 family inet address 10.38.0.13/30
      set interfaces ge-1/0/2 unit 0 family mpls
      set interfaces ge-1/0/3 unit 0 family inet address 10.32.0.17/30
      set interfaces ge-1/0/3 unit 0 family mpls
      set interfaces ge-1/0/5 unit 0 family inet address 192.0.2.3/24
      set interfaces ge-1/0/5 unit 0 family mpls
      set interfaces ge-1/1/0 unit 0 family inet address 10.38.0.2/30
      set interfaces ge-1/1/0 unit 0 family mpls
      set interfaces ge-1/2/0 unit 0 family inet address 10.32.0.2/30
      set interfaces ge-1/2/0 unit 0 family mpls
      set interfaces lo0 unit 0 family inet address 10.255.104.134/32
      set chassis network-services enhanced-ip
      set routing-options forwarding-table chained-composite-next-hop ingress l3vpn
      set routing-instances vpn-a instance-type vrf
      set routing-instances vpn-a interface ge-1/0/5.0

```

```

set routing-instances vpn-a route-distinguisher 200:2
set routing-instances vpn-a vrf-target target:200:1
set routing-instances vpn-a protocols bgp group CE type external
set routing-instances vpn-a protocols bgp group CE peer-as 300
set routing-instances vpn-a protocols bgp group CE neighbor 192.0.2.3
set protocols mpls interface 10.38.0.2/30
set protocols mpls interface 10.32.0.2/30
set protocols mpls interface 10.38.0.13/30
set protocols mpls interface 10.38.0.17/30
set protocols bgp group PEs type internal
set protocols bgp group PEs local-address 10.255.104.134
set protocols bgp group PEs family inet unicast
set protocols bgp group PEs family inet-vpn unicast
set protocols bgp group PEs neighbor 10.255.104.133
set protocols bgp group PEs neighbor 10.255.104.135
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set routing-options autonomous-system 200

```

```

P    set interfaces ge-2/0/1 unit 0 family inet address 10.38.0.6/30
    set interfaces ge-2/0/1 unit 0 family mpls
    set interfaces ge-2/0/2 unit 0 family inet address 10.38.0.14/30
    set interfaces ge-2/0/2 unit 0 family mpls
    set interfaces ge-2/0/3 unit 0 family inet address 10.38.0.21/30
    set interfaces ge-2/0/3 unit 0 family mpls
    set interfaces lo0 unit 0 family inet address 10.255.104.136/32
    set protocols mpls interface 10.38.0.6/30
    set protocols mpls interface 10.38.0.14/30
    set protocols mpls interface 10.38.0.21/30
    set protocols bgp group PEs type internal
    set protocols bgp group PEs local-address 10.255.104.136
    set protocols bgp group PEs family inet unicast
    set protocols bgp group PEs family inet-vpn unicast
    set protocols bgp group PEs neighbor 10.255.104.133
    set protocols ospf area 0.0.0.0 interface all
    set protocols ospf area 0.0.0.0 interface fxp0.0 disable
    set protocols ospf area 0.0.0.0 interface lo0.0 passive
    set protocols ldp interface all
    set protocols ldp interface fxp0.0 disable
    set routing-options autonomous-system 200

```

```

PE3  set interfaces ge-3/0/0 unit 0 family inet address 10.38.0.10/30r0-r3
    set interfaces ge-3/0/0 unit 0 family mpls
    set interfaces ge-3/0/1 unit 0 family inet address 10.38.0.18/30r0-r1-2
    set interfaces ge-3/0/1 unit 0 family mpls
    set interfaces ge-3/0/2 unit 0 family inet address 10.38.0.22/30
    set interfaces ge-3/0/2 unit 0 family mpls
    set interfaces ge-3/0/5 unit 0 family inet address 192.0.2.6/24r0-r1-1
    set interfaces ge-3/0/5 unit 0 family mpls
    set interfaces lo0 unit 0 family inet address 10.255.104.135/32
    set chassis network-services enhanced-mode
    set routing-options forwarding-table chained-composite-next-hop ingress l3vpn

```

```

set routing-options autonomous-system 200
set routing-instances vpn-a instance-type vrf
set routing-instances vpn-a interface ge-3/0/5.0
set routing-instances vpn-a route-distinguisher 200:3
set routing-instances vpn-a vrf-target target:200:1
set routing-instances vpn-a protocols bgp group CE type external
set routing-instances vpn-a protocols bgp group CE peer-as 300
set routing-instances vpn-a protocols bgp group CE neighbor 192.0.2.5
set protocols mpls interface 10.38.0.10/30
set protocols mpls interface 10.38.0.18/30
set protocols mpls interface 10.38.0.22/30
set protocols bgp group PEs type internal
set protocols bgp group PEs local-address 10.255.104.135
set protocols bgp group PEs family inet unicast
set protocols bgp group PEs family inet-vpn unicast
set protocols bgp group PEs neighbor 10.255.104.133
set protocols bgp group PEs neighbor 10.255.104.134
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable

```

```

CE2  set interfaces ge-2/2/2 unit 0 family inet address 192.0.2.4/24
      set interfaces ge-2/2/2 unit 0 family mpls
      set interfaces ge-2/2/3 unit 0 family inet address 192.0.2.5/24
      set interfaces ge-2/2/3 unit 0 family mpls
      set interfaces lo0 unit 0 family inet address 192.0.2.7/24
      set protocols bgp group PE type external
      set protocols bgp group PE metric-out 50
      set protocols bgp group PE peer-as 200
      set protocols bgp group PE export s2b
      set protocols bgp group PE neighbor 192.0.2.4
      set protocols bgp group PE neighbor 192.0.2.5
      set policy-options policy-statement s2b from protocol direct
      set policy-options policy-statement s2b then accept
      set routing-options autonomous-system 300

```

Configuring Multipath Layer 3 VPN with Chained Composite Next Hop

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 basic Layer 3 VPN with chained composite next hop on the PE1 router:



NOTE: Repeat this procedure for the PE2 and PE3 routers in the MPLS domain, after modifying the appropriate interface names, addresses, and any other parameters for each router.

1. Configure the interfaces on the PE1 router.

PE1 to CE1

```
[edit interfaces]
user@PE1 # set ge-0/1/1 unit 0 family inet address 192.0.2.1/24
user@PE1 # set ge-0/1/1 unit 0 family mpls
```

PE1 to PE2

```
[edit interfaces]
user@PE1 # set ge-0/0/1 unit 0 family inet address 10.38.0.1/30
user@PE1 # set ge-0/0/1 unit 0 family mpls

user@PE1 # set ge-0/0/2 unit 0 family inet address 10.38.0.5/30
user@PE1 # set ge-0/0/2 unit 0 family mpls
```

PE1 to P

```
[edit interfaces]
user@PE1 # set ge-0/0/4 unit 0 family inet address 10.32.0.1/30
user@PE1 # set ge-0/0/4 unit 0 family mpls
```

PE1 to PE3

```
[edit interfaces]
user@PE1 # set ge-0/0/3 unit 0 family inet address 10.38.0.9/30
user@PE1 # set ge-0/0/3 unit 0 family mpls
```

Loopback interface

```
[edit interfaces]
user@PE1 # set lo0 unit 0 family inet address 10.255.104.133/32
```

2. Enable enhanced IP mode on the PE1 chassis.

```
[edit chassis]
user@PE1# set network-services enhanced-ip
```

3. Enable chained composite next hop on the global Layer 3 VPN.

```
[edit routing-options]
user@PE1# set forwarding-table chained-composite-next-hop ingress l3vpn
```

4. Configure the autonomous system for PE1.

```
[edit routing-options]
user@PE1# set autonomous-system 200
```

5. Export the policy configured for load balancing.

```
[edit routing-options]
user@PE1# set forwarding-table export lbpp
```

6. Configure MPLS on the PE1 interfaces connecting to the P router and other PE routers.

```
[edit protocols]
user@PE1# set mpls interface 10.38.0.1/30
user@PE1# set mpls interface 10.32.0.1/30
user@PE1# set mpls interface 10.38.0.5/30
user@PE1# set mpls interface 10.38.0.9/30
```

7. Configure the IBGP group for PE1 to peer with the PE2 and PE3 routers.

```
[edit protocols]
user@PE1# set bgp group PEs type internal
user@PE1# set bgp group PEs local-address 10.255.104.133
user@PE1# set bgp group PEs family inet unicast
user@PE1# set bgp group PEs family inet-vpn unicast
user@PE1# set bgp group PEs neighbor 10.255.104.134 local-preference 200
user@PE1# set bgp group PEs neighbor 10.255.104.135
```

8. Configure OSPF with traffic engineering capability on all the interfaces of PE1, excluding the management interface.

```
[edit protocols]
user@PE1# set ospf area 0.0.0.0 interface all
user@PE1# set ospf area 0.0.0.0 interface fxp0.0 disable
user@PE1# set ospf area 0.0.0.0 interface lo0.0 passive
```

9. Configure LDP on all the interfaces of PE1, excluding the management interface.

```
[edit protocols]
user@PE1# set ldp interface all
user@PE1# set ldp interface fxp0.0 disable
```

10. Configure a policy to load-balance traffic on a per packet basis.

```
[edit policy-options]
user@PE1# set policy-statement lbpp then load-balance per-packet
```

11. Configure a VRF routing instance on the CE1-facing interface of PE1.

```
[edit routing-instances]
user@PE1# set vpn-a instance-type vrf
user@PE1# set vpn-a interface ge-0/1/1.0
```

12. Configure the routing instance parameters.

```
[edit routing-instances]
user@PE1# set vpn-a route-distinguisher 200:1
user@PE1# set vpn-a vrf-target target:200:1
user@PE1# set vpn-a vrf-table-label
```

13. Configure an EBGp group for the routing instance, so PE1 can peer with CE1.

```
[edit routing-instances]
user@PE1# set vpn-a protocols bgp group CE type external
user@PE1# set vpn-a protocols bgp group CE peer-as 100
user@PE1# set vpn-a protocols bgp group CE neighbor 192.0.2.2
```

Results

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

```
PE1 user@PE1# show chassis
network-services enhanced-ip;

user@PE1# show interfaces
```

```
ge-0/0/1 {
  unit 0 {
    family inet {
      address 10.38.0.1/30;
    }
    family mpls;
  }
}
ge-0/0/2 {
  unit 0 {
    family inet {
      address 10.38.0.5/30;
    }
    family mpls;
  }
}
ge-0/0/3 {
  unit 0 {
    family inet {
      address 10.38.0.9/30;
    }
    family mpls;
  }
}
ge-0/0/4 {
  unit 0 {
    family inet {
      address 10.32.0.1/30;
    }
    family mpls;
  }
}
ge-0/1/1 {
  unit 0 {
    family inet {
      address 192.0.2.1/24;
    }
    family mpls;
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.255.104.133/32;
    }
  }
}

user@PE1# show protocols
mpls {
  interface 10.38.0.1/30;
  interface 10.32.0.1/30;
  interface 10.38.0.5/30;
  interface 10.38.0.9/30;
}
bgp {
```



```

group PEs {
  type internal;
  local-address 10.255.104.133;
  family inet {
    unicast;
  }
  family inet-vpn {
    unicast;
  }
  neighbor 10.255.104.134 {
    local-preference 200;
  }
  neighbor 10.255.104.135;
}
}
ospf {
  area 0.0.0.0 {
    interface all;
    interface fxp0.0 {
      disable;
    }
    interface lo0.0 {
      passive;
    }
  }
}
}
ldp {
  interface all;
  interface fxp0.0 {
    disable;
  }
}
}

user@PE1# show routing-options
autonomous-system 200;
forwarding-table {
  export lbpp;
  chained-composite-next-hop {
    ingress {
      l3vpn;
    }
  }
}
}

user@PE1# show routing-instances
vpn-a {
  instance-type vrf;
  interface ge-0/1/1.0;
  route-distinguisher 200:1;
  vrf-target target:200:1;
  vrf-table-label;
  protocols {
    bgp {
      group CE {
        type external;
        peer-as 100;
        neighbor 192.0.2.2;

```

```
    }  
  }  
}  
  
user@PE1# show policy-options  
policy-statement lbpp {  
  then {  
    load-balance per-packet;  
  }  
}
```

Verification

Confirm that the configuration is working properly.

- [Verifying the Routes on page 94](#)
- [Verifying Chained Next Hop on Direct PE-PE Connection on page 96](#)

Verifying the Routes

Purpose Verify that the Layer 3 VPN prefixes toward PE1-PE2 point to composite next hops.

Action From operational mode, run the **show route 192.0.2.7 table vpn-a extensive** command.

```
user@PE1> show route 192.0.2.7 table vpn-a extensive
```

```
vpn-a.inet.0: 7 destinations, 10 routes (7 active, 0 holddown, 0 hidden)
192.0.2.7/24 (2 entries, 1 announced)
TSI:
KRT in-kernel 192.0.2.7/24 -> {composite(720)}
Page 0 idx 0, (group CE type External) Type 1 val 938eaa8 (adv_entry)
  Advertised metrics:
    Nexthop: Self
    AS path: [200] 300 I
    Communities: target:200:1
Path 192.0.2.7 from 10.255.104.133 Vector len 4. Val: 0
  *BGP Preference: 170/-101
    Route Distinguisher: 200:2
    Next hop type: Indirect
    Address: 0x9391654
    Next-hop reference count: 12
    Source: 10.255.104.133
    Next hop type: Router, Next hop index: 1048580
    Next hop: 10.32.0.2 via ge-0/0/2.0
    Session Id: 0x1
    Next hop: 10.38.0.2 via ge-0/0/1.0, selected
    Session Id: 0x3
    Protocol next hop: 10.255.104.133
    Push 300192
    Composite next hop: 0x93918a4 718 INH Session ID: 0x9
    Indirect next hop: 0x941c000 1048581 INH Session ID: 0x9
    State: <Secondary Active Int Ext ProtectionCand>
    Local AS: 200 Peer AS: 200
    Age: 28 Metric: 50 Metric2: 1
    Validation State: unverified
    Task: BGP_200.10.255.104.133+57173
    Announcement bits (2): 0-KRT 1-BGP_RT_Background
    AS path: 300 I
    Communities: target:200:1
    Import Accepted
    VPN Label: 300192
    Localpref: 100
    Router ID: 10.255.104.133
    Primary Routing Table bgp.l3vpn.0
    Composite next hops: 1
      Protocol next hop: 10.255.104.133 Metric: 1
      Push 300192
      Composite next hop: 0x93918a4 718 INH Session ID: 0x9
      Indirect next hop: 0x941c000 1048581 INH Session ID:
0x9
      Indirect path forwarding next hops: 2
        Next hop type: Router
        Next hop: 10.32.0.2 via ge-1/0/0.0
        Session Id: 0x1
        Next hop: 10.38.0.2 via ge-1/1/2.0
        Session Id: 0x3
      10.255.104.133/32 Originating RIB: inet.3
        Metric: 1 Node path count: 1
        Forwarding nexthops: 2
          Nexthop: 10.32.0.2 via ge-0/0/2.0
    BGP Preference: 170/-101
```

```

Route Distinguisher: 200:3
Next hop type: Indirect
Address: 0x9391608
Next-hop reference count: 9
Source: 10.255.104.131
Next hop type: Router, Next hop index: 722
Next hop: 10.38.0.10 via ge-0/0/1.0, selected
Session Id: 0x4
Protocol next hop: 10.255.104.131
Push 299936
Composite next hop: 0x9391690 723 INH Session ID: 0xb
Indirect next hop: 0x941c0fc 1048583 INH Session ID: 0xb
State: <Secondary NotBest Int Ext ProtectionCand>
Inactive reason: Not Best in its group - Router ID
Local AS: 200 Peer AS: 200
Age: 28 Metric: 50 Metric2: 1
Validation State: unverified
Task: BGP_200.10.255.104.131+63797
AS path: 300 I
Communities: target:200:1
Import Accepted
VPN Label: 299936
Localpref: 100
Router ID: 10.255.104.131
Primary Routing Table bgp.l3vpn.0
Composite next hops: 1
    Protocol next hop: 10.255.104.131 Metric: 1
    Push 299936
    Composite next hop: 0x9391690 723 INH Session ID: 0xb
    Indirect next hop: 0x941c0fc 1048583 INH Session ID:
0xb
        Indirect path forwarding next hops: 1
            Next hop type: Router
            Next hop: 10.38.0.10 via ge-1/0/2.0
            Session Id: 0x4
10.255.104.131/32 Originating RIB: inet.3
Metric: 1 Node path count: 1
Forwarding nexthops: 1
Nexthop: 10.38.0.10 via ge-1/0/2.0

```

Meaning The PE2 router is the composite next hop for PE1 to reach CE2.

Verifying Chained Next Hop on Direct PE-PE Connection

Purpose Verify that chained next hop is generated for direct PE-PE connection on CE1.

Action From operational mode, run the **ping** command.

```

user@CE1> ping 192.0.2.4
!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss

```

Meaning Chained composite next hop is enabled for the PE1 to PE2 connection.

- Related Documentation**
- [Chained Composite Next Hops for Transit Devices for VPNs on page 83](#)

CHAPTER 6

Configuring Graceful Restart for VPNs

- [VPN Graceful Restart on page 99](#)
- [Configuring Graceful Restart for VPNs on page 100](#)
- [Enabling Unicast Reverse-Path Forwarding Check for VPNs on page 102](#)
- [Example: Configuring Unicast Reverse-Path-Forwarding Check on page 103](#)

VPN Graceful Restart

VPN graceful restart allows a router whose VPN control plane is undergoing a restart to continue to forward traffic while recovering its state from neighboring routers. Without graceful restart, a control plane restart disrupts any VPN services provided by the router.

For VPN graceful restart to function properly, the following items need to be configured on the PE router:

- BGP graceful restart must be active on the PE-to-PE sessions carrying any service-signaling data in the session's network layer reachability information (NLRI).
- OSPF, IS-IS, LDP, and RSVP graceful restart must be active, because routes added by these protocols are used to resolve VPN NLRIs.
- For other protocols (static, Routing Information Protocol [RIP], and so on), graceful restart functionality must also be active when these protocols are run between the PE and CE routers. Layer 2 VPNs do not rely on this because protocols are not configured between the PE and CE routers.

In VPN graceful restart, a restarting router completes the following procedures:

- Waits for all the BGP NLRI information from other PE routers before it starts advertising routes to its CE routers.
- Waits for all protocols in all routing instances to converge (or finish graceful restart) before sending CE router information to the other PE routers.

- Waits for all routing instance information (whether it is local configuration or advertisements from a remote peer router) to be processed before sending it to the other PE routers.
- Preserves all forwarding state information in the MPLS routing tables until new labels and transit routes are allocated and then advertises them to other PE routers (and CE routers in carrier-of-carriers VPNs).

Graceful restart is supported on Layer 2 VPNs, Layer 3 VPNs, and virtual-router routing instances.

Configuring Graceful Restart for VPNs

You can configure graceful restart to enable a router to pass through intermediate convergence states that are hidden from the rest of the network. Graceful restart allows a router whose VPN control plane is undergoing a restart (restarting router) to continue to forward traffic while recovering its state from neighboring routers (helper routers).

The restarting router requests a grace period from the neighbor or peer, which can then cooperate with the restarting router. When a restart event occurs and graceful restart is enabled, the restarting router can still forward traffic during the restart period, and convergence in the network is not disrupted. The helper routers hide the restart event from other devices not directly connected to the restarting router. In other words, the restart is not visible to the rest of the network, and the restarting router is not removed from the network topology.

Without graceful restart, a control plane restart disrupts any VPN services provided by the router. Graceful restart is supported on Layer 2 VPNs, Layer 3 VPNs, virtual-router routing instances, and VPLS.

The graceful restart request occurs only if the following conditions are met:

- The network topology is stable.
- The neighbor or peer routers cooperate.
- The restarting router is not already cooperating with another restart already in progress.
- The grace period does not expire.

Before you begin:

- Configure the devices for network communication.
- Configure the device interfaces.

Graceful restart is disabled by default. To enable VPN graceful restart:

1. Configure graceful restart globally.

```
[edit routing-options]  
user@host# set graceful-restart
```


**NOTE:**

- Graceful restart can be enabled on logical systems. To configure graceful restart globally, include the `graceful-restart` statement at the `[edit logical-systems logical-system-name routing-options]` or the `[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options]` hierarchy levels.
- To disable graceful restart globally, include the `disable` statement at the `[edit routing-options graceful-restart]` hierarchy level.

For example:

```
[edit routing-options]
user@host# set graceful-restart disable
```

2. Enable or disable graceful restart on a per-protocol, per-group, or per-neighbor basis, depending on the specific protocol, where the most specific definition is used.

```
[edit protocols]
user@host# set bgp graceful-restart
user@host# set bgp group group-name type internal local-address local-ip-address
neighbor neighbor1-address
user@host# set bgp group group-name type internal local-address local-ip-address
neighbor neighbor2-address graceful-restart disable
```

3. Configure graceful restart for Layer 3 VPNs for all routing and MPLS-related protocols within a routing instance. Because you can configure multi-instance BGP and multi-instance LDP, graceful restart for a carrier-of-carriers scenario is supported.

```
[edit routing-instance]
user@host# set routing-instance-name routing-options graceful-restart
```

**NOTE:**

- To disable graceful restart globally, include the `disable` statement at the `[edit routing-instances routing-instance-name routing-options graceful-restart]` hierarchy level.

For example:

```
[edit routing-instances]
user@host# set instance1 routing-options graceful-restart disable
```

- To disable graceful restart for individual protocols, include the `disable` statement at the `[edit routing-instances routing-instance-name protocols protocol-name graceful-restart]` hierarchy level.

For example:

```
[edit routing-instances]
user@host# set instance1 protocols ospf graceful-restart disable
```

4. Configure the duration of the graceful restart period for the routing instance.

```
[edit routing-options]
user@host# set graceful-restart restart-duration seconds
```

The **restart-duration** option sets the period of time that the router waits for a graceful restart to be completed. You can configure a time between 1 through 600 seconds. The default value is 300 seconds. At the end of the configured time period, the router performs a standard restart without recovering its state from the neighboring routers. This disrupts VPN services, but is probably necessary if the router is not functioning normally.



NOTE: You can include the **restart-duration** option at either the global or routing instance level. The routing instance value overrides the global value if both are configured.

**Related
Documentation**

- *Graceful Restart and Layer 2 and Layer 3 VPNs*
- *Graceful Restart System Requirements*
- *Graceful Restart Concepts*
- *Verifying Graceful Restart Operation*

Enabling Unicast Reverse-Path Forwarding Check for VPNs

IP spoofing may occur during a denial-of-service (DoS) attack. IP spoofing allows an intruder to pass IP packets to a destination as genuine traffic, when in fact the packets are not actually meant for the destination. This type of spoofing is harmful because it consumes the destination's resources.

Unicast reverse-path forwarding (RPF) check is a tool to reduce forwarding of IP packets that may be spoofing an address. A unicast RPF check performs a route table lookup on an IP packet's source address, and checks the incoming interface. The router determines whether the packet is arriving from a path that the sender would use to reach the destination. If the packet is from a valid path, the router forwards the packet to the destination address. If it is not from a valid path, the router discards the packet. Unicast RPF is supported for the IPv4 and IPv6 protocol families, as well as for the virtual private network (VPN) address family. You can also enable unicast RPF within a VPN routing instance.

To enable unicast RPF check, include the **unicast-reverse-path** statement:

unicast-reverse-path (active-paths | feasible-paths);

For a list of hierarchy levels at which you can configure this statement, see the statement summary section for this statement.

To consider only active paths during the unicast RPF check, include the **active-paths** option. To consider all feasible paths during the unicast RPF check, include the **feasible-paths** option.

For more information about how to configure the **unicast-reverse-path** statement, see [“Example: Configuring Unicast Reverse-Path-Forwarding Check” on page 103](#) and .

- Related Documentation**
- [Example: Configuring Unicast Reverse-Path-Forwarding Check on page 103](#)

Example: Configuring Unicast Reverse-Path-Forwarding Check

- [Understanding Unicast Reverse Path Forwarding on page 103](#)
- [Example: Configuring Unicast Reverse-Path-Forwarding Check on page 103](#)

Understanding Unicast Reverse Path Forwarding

IP spoofing can occur during a denial-of-service (DoS) attack. IP spoofing allows an intruder to pass IP packets to a destination as genuine traffic, when in fact the packets are not actually meant for the destination. This type of spoofing is harmful because it consumes the destination's resources.

A unicast reverse-path-forwarding (RPF) check is a tool to reduce forwarding of IP packets that might be spoofing an address. A unicast RPF check performs a route table lookup on an IP packet's source address, and checks the incoming interface. The router or switch determines whether the packet is arriving from a path that the sender would use to reach the destination. If the packet is from a valid path, the router or switch forwards the packet to the destination address. If it is not from a valid path, the router or switch discards the packet. Unicast RPF is supported for the IPv4 and IPv6 protocol families, as well as for the virtual private network (VPN) address family.



NOTE: Reverse path forwarding is not supported on the interfaces you configure as tunnel sources. This affects only the transit packets exiting the tunnel.

Example: Configuring Unicast Reverse-Path-Forwarding Check

Unicast reverse path forwarding (RPF) helps protect against DoS and DDoS attacks by verifying the unicast source address of each packet that arrives on an ingress interface where unicast RPF is enabled.

This example shows how to help defend ingress interfaces against denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks by configuring unicast RPF to filter incoming traffic.

- [Requirements on page 103](#)
- [Overview on page 104](#)
- [Configuration on page 104](#)
- [Verification on page 110](#)

Requirements

In this example, no special configuration beyond device initialization is required.

Overview

Large amounts of unauthorized traffic such as attempts to flood a network with fake (bogus) service requests in a DoS attack can consume network resources and deny service to legitimate users. One way to help prevent DoS and DDoS attacks is to verify that incoming traffic originates from legitimate network sources.

Unicast RPF helps ensure that a traffic source is legitimate (authorized) by comparing the source address of each packet that arrives on an interface to the forwarding table entry for its source address. If the device uses the same interface that the packet arrived on to reply to the packet's source, this verifies that the packet originated from an authorized source, and the device forwards the packet. If the device does not use the same interface that the packet arrived on to reply to the packet's source, the packet might have originated from an unauthorized source, and the device discards the packet.

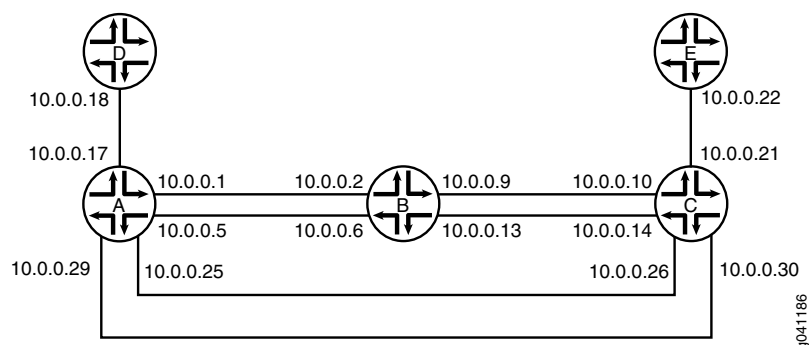
In this example, Device B has unicast RPF configured. Device A is using OSPF to advertise a prefix for the link that connects to Device D. OSPF is enabled on the links between Device B and Device C and the links between Device A and Device C, but not on the links between Device A and Device B. Therefore, Device B learns about the route to Device D through Device C.

If ingress filtering is used in an environment where DHCP or BOOTP is used, it should be ensured that the packets with a source address of 0.0.0.0 and a destination address of 255.255.255.255 are allowed to reach the relay agent in routers when appropriate.

This example also includes a fail filter. When a packet fails the unicast RPF check, the fail filter is evaluated to determine if the packet should be accepted anyway. The fail filter in this example allows Device B's interfaces to accept Dynamic Host Configuration Protocol (DHCP) packets. The filter accepts all packets with a source address of 0.0.0.0 and a destination address of 255.255.255.255.

Figure 8 on page 104 shows the sample network.

Figure 8: Unicast RPF Sample Topoolgy



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 A	<pre> set interfaces fe-1/2/0 unit 1 family inet address 10.0.0.1/30 set interfaces fe-0/0/2 unit 5 family inet address 10.0.0.5/30 set interfaces fe-0/0/1 unit 17 family inet address 10.0.0.17/30 set interfaces fe-0/1/1 unit 25 family inet address 10.0.0.25/30 set interfaces fe-1/1/1 unit 29 family inet address 10.0.0.29/30 set protocols ospf export send-direct set protocols ospf area 0.0.0.0 interface fe-0/1/1.25 set protocols ospf area 0.0.0.0 interface fe-1/1/1.29 set policy-options policy-statement send-direct from protocol direct set policy-options policy-statement send-direct from route-filter 10.0.0.16/30 exact set policy-options policy-statement send-direct then accept </pre>
Device B	<pre> set interfaces fe-1/2/0 unit 2 family inet rpf-check fail-filter rpf-special-case-dhcp set interfaces fe-1/2/0 unit 2 family inet address 10.0.0.2/30 set interfaces fe-1/1/1 unit 6 family inet rpf-check fail-filter rpf-special-case-dhcp set interfaces fe-1/1/1 unit 6 family inet address 10.0.0.6/30 set interfaces fe-0/1/1 unit 9 family inet rpf-check fail-filter rpf-special-case-dhcp set interfaces fe-0/1/1 unit 9 family inet address 10.0.0.9/30 set interfaces fe-0/1/0 unit 13 family inet rpf-check fail-filter rpf-special-case-dhcp set interfaces fe-0/1/0 unit 13 family inet address 10.0.0.13/30 set protocols ospf area 0.0.0.0 interface fe-0/1/1.9 set protocols ospf area 0.0.0.0 interface fe-0/1/0.13 set routing-options forwarding-table unicast-reverse-path active-paths set firewall filter rpf-special-case-dhcp term allow-dhcp from source-address 0.0.0.0/32 set firewall filter rpf-special-case-dhcp term allow-dhcp from destination-address 255.255.255.255/32 set firewall filter rpf-special-case-dhcp term allow-dhcp then count rpf-dhcp-traffic set firewall filter rpf-special-case-dhcp term allow-dhcp then accept set firewall filter rpf-special-case-dhcp term default then log set firewall filter rpf-special-case-dhcp term default then reject </pre>
Device C	<pre> set interfaces fe-1/2/0 unit 10 family inet address 10.0.0.10/30 set interfaces fe-0/0/2 unit 14 family inet address 10.0.0.14/30 set interfaces fe-1/0/2 unit 21 family inet address 10.0.0.21/30 set interfaces fe-1/2/2 unit 26 family inet address 10.0.0.26/30 set interfaces fe-1/2/1 unit 30 family inet address 10.0.0.30/30 set protocols ospf area 0.0.0.0 interface fe-1/2/0.10 set protocols ospf area 0.0.0.0 interface fe-0/0/2.14 set protocols ospf area 0.0.0.0 interface fe-1/2/2.26 set protocols ospf area 0.0.0.0 interface fe-1/2/1.30 </pre>
Device D	<pre> set interfaces fe-1/2/0 unit 18 family inet address 10.0.0.18/30 </pre>
Device E	<pre> set interfaces fe-1/2/0 unit 22 family inet address 10.0.0.22/30 </pre>

Configuring Device A

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 Device A:

1. Configure the interfaces.

```
[edit interfaces]
user@A# set fe-1/2/0 unit 1 family inet address 10.0.0.1/30

user@A# set fe-0/0/2 unit 5 family inet address 10.0.0.5/30

user@A# set fe-0/0/1 unit 17 family inet address 10.0.0.17/30

user@A# set fe-0/1/1 unit 25 family inet address 10.0.0.25/30

user@A# set fe-1/1/1 unit 29 family inet address 10.0.0.29/30
```
2. Configure OSPF.

```
[edit protocols ospf]
user@A# set export send-direct
user@A# set area 0.0.0.0 interface fe-0/1/1.25
user@A# set area 0.0.0.0 interface fe-1/1/1.29
```
3. Configure the routing policy.

```
[edit policy-options policy-statement send-direct]
user@A# set from protocol direct
user@A# set from route-filter 10.0.0.16/30 exact
user@A# set then accept
```
4. If you are done configuring Device A, commit the configuration.

```
[edit]
user@A# commit
```

Configuring Device B

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 Device B:

1. Configure the interfaces.

```
[edit interfaces]
user@B# set fe-1/2/0 unit 2 family inet address 10.0.0.2/30

user@B# set fe-1/1/1 unit 6 family inet address 10.0.0.6/30

user@B# set fe-0/1/1 unit 9 family inet address 10.0.0.9/30
```

- ```

user@B# set fe-0/1/0 unit 13 family inet address 10.0.0.13/30

```
2. Configure OSPF.
 

```

[edit protocols ospf area 0.0.0.0]
user@B# set interface fe-0/1/1.9
user@B# set interface fe-0/1/0.13

```
  3. Configure unicast RPF, and apply the optional fail filter.
 

```

[edit interfaces]
user@B# set fe-1/2/0 unit 2 family inet rpf-check fail-filter rpf-special-case-dhcp

user@B# set fe-1/1/1 unit 6 family inet rpf-check fail-filter rpf-special-case-dhcp

user@B# set fe-0/1/1 unit 9 family inet rpf-check fail-filter rpf-special-case-dhcp

user@B# set fe-0/1/0 unit 13 family inet rpf-check fail-filter rpf-special-case-dhcp

```
  4. (Optional) Configure the fail filter that gets evaluated if a packet fails the RPF check.
 

```

[edit firewall filter rpf-special-case-dhcp]
user@B# set term allow-dhcp from source-address 0.0.0.0/32
user@B# set term allow-dhcp from destination-address 255.255.255.255/32
user@B# set term allow-dhcp then count rpf-dhcp-traffic
user@B# set term allow-dhcp then accept
user@B# set term default then log
user@B# set term default then reject

```
  5. (Optional) Configure only active paths to be considered in the RPF check.  
This is the default behavior.
 

```

[edit routing-options forwarding-table]
user@B# set unicast-reverse-path active-paths

```
  6. If you are done configuring Device B, commit the configuration.
 

```

[edit]
user@B# commit

```

### Results

Confirm your configuration by issuing the **show firewall**, **show interfaces**, **show protocols**, **show routing-options**, and **show policy-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```

Device A user@A# show interfaces
fe-1/2/0 {
 unit 1 {
 family inet {
 address 10.0.0.1/30;
 }
 }
}
fe-0/0/2 {
 unit 5 {

```

```
 family inet {
 address 10.0.0.5/30;
 }
 }
}
fe-0/0/1 {
 unit 17 {
 family inet {
 address 10.0.0.17/30;
 }
 }
}
fe-0/1/1 {
 unit 25 {
 family inet {
 address 10.0.0.25/30;
 }
 }
}
fe-1/1/1 {
 unit 29 {
 family inet {
 address 10.0.0.29/30;
 }
 }
}
}
```

user@A# show protocols

```
ospf {
 export send-direct;
 area 0.0.0.0 {
 interface fe-0/1/1.25;
 interface fe-1/1/1.29;
 }
}
```

user@A# show policy-options

```
policy-statement send-direct {
 from {
 protocol direct;
 route-filter 10.0.0.16/30 exact;
 }
 then accept;
}
```

#### Device B

user@B# show firewall

```
filter rpf-special-case-dhcp {
 term allow-dhcp {
 from {
 source-address {
 0.0.0.0/32;
 }
 destination-address {
 255.255.255.255/32;
 }
 }
 destination-address {
```



```

 255.255.255.255/32;
 }
}
then {
 count rpf-dhcp-traffic;
 accept;
}
}
term default {
 then {
 log;
 reject;
 }
}
}
}
user@B# show interfaces
fe-1/2/0 {
 unit 2 {
 family inet {
 rpf-check fail-filter rpf-special-case-dhcp;
 address 10.0.0.2/30;
 }
 }
}
fe-1/1/1 {
 unit 6 {
 family inet {
 rpf-check fail-filter rpf-special-case-dhcp;
 address 10.0.0.6/30;
 }
 }
}
fe-0/1/1 {
 unit 9 {
 family inet {
 rpf-check fail-filter rpf-special-case-dhcp;
 address 10.0.0.9/30;
 }
 }
}
fe-0/1/0 {
 unit 13 {
 family inet {
 rpf-check fail-filter rpf-special-case-dhcp;
 address 10.0.0.13/30;
 }
 }
}
}
user@B# show protocols
ospf {
 area 0.0.0.0 {
 interface fe-0/1/1.9;
 interface fe-0/1/0.13;
 }
}
}

```

```
user@B# show routing-options
forwarding-table {
 unicast-reverse-path active-paths;
}
```

Enter the configurations on Device C, Device D, and Device E, as shown in [“CLI Quick Configuration” on page 104](#).

---

### Verification

Confirm that the configuration is working properly.

- [Confirm That Unicast RPF Is Enabled on page 110](#)
- [Confirm That the Source Addresses Are Blocked on page 110](#)
- [Confirm That the Source Addresses Are Unblocked on page 111](#)

#### *Confirm That Unicast RPF Is Enabled*

**Purpose** Make sure that the interfaces on Device B have unicast RPF enabled.

**Action** user@B> show interfaces fe-0/1/0.13 extensive  
Logical interface fe-0/1/0.13 (Index 73) (SNMP ifIndex 553) (Generation 208)  
Flags: SNMP-Traps 0x4000 Encapsulation: ENET2  
Traffic statistics:  
Input bytes : 999390  
Output bytes : 1230122  
Input packets: 12563  
Output packets: 12613  
Local statistics:  
Input bytes : 998994  
Output bytes : 1230122  
Input packets: 12563  
Output packets: 12613  
Transit statistics:  
Input bytes : 396 0 bps  
Output bytes : 0 0 bps  
Input packets: 0 0 pps  
Output packets: 0 0 pps  
Protocol inet, MTU: 1500, Generation: 289, Route table: 22  
Flags: Sendbcst-pkt-to-re, uRPF  
RPF Failures: Packets: 0, Bytes: 0  
Addresses, Flags: Is-Preferred Is-Primary  
Destination: 10.0.0.12/30, Local: 10.0.0.13, Broadcast: 10.0.0.15,  
Generation: 241

**Meaning** The uRPF flag confirms that unicast RPF is enabled on this interface.

#### *Confirm That the Source Addresses Are Blocked*

**Purpose** Use the **ping** command to make sure that Device B blocks traffic from unexpected source addresses.

**Action** From Device A, ping Device B's interfaces, using 10.0.0.17 as the source address.

```
user@A> ping 10.0.0.6 source 10.0.0.17
PING 10.0.0.6 (10.0.0.6): 56 data bytes
^C
--- 10.0.0.6 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
```

**Meaning** As expected, the ping operation fails.

#### *Confirm That the Source Addresses Are Unblocked*

**Purpose** Use the **ping** command to make sure that Device B does not block traffic when the RPF check is deactivated.

**Action**

1. Deactivate the RPF check on one of the interfaces.
2. Rerun the ping operation.

```
user@B> deactivate interfaces fe-1/1/1.6 family inet rpf-check

user@A> ping 10.0.0.6 source 10.0.0.17
PING 10.0.0.2 (10.0.0.2): 56 data bytes
64 bytes from 10.0.0.2: icmp_seq=0 ttl=63 time=1.316 ms
64 bytes from 10.0.0.2: icmp_seq=1 ttl=63 time=1.263 ms
^C
--- 10.0.0.2 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.263/1.289/1.316/0.027 ms
```

**Meaning** As expected, the ping operation succeeds.

**Related Documentation**

- *Example: Enabling Indirect Next Hops on the Packet Forwarding Engine*



## CHAPTER 7

# Configuring Class of Service for VPNs

- [VPNs and Class of Service on page 113](#)
- [Rewriting Class of Service Markers and VPNs on page 113](#)

### VPNs and Class of Service

---

You can configure Junos class-of-service (CoS) features to provide multiple classes of service for VPNs. The CoS features are supported on Layer2 VPNs, Layer 3 VPNs, and VPLS. On the router, you can configure multiple forwarding classes for transmitting packets, define which packets are placed into each output queue, schedule the transmission service level for each queue, and manage congestion using a random early detection (RED) algorithm.

VPNs use the standard CoS configuration. For information about how to configure CoS, see the *Class of Service Feature Guide for Routing Devices*.

### Rewriting Class of Service Markers and VPNs

---

A marker reads the current forwarding class and loss priority information associated with a packet and finds the chosen code point from a table. It then writes the code point information into the packet header. Entries in a marker configuration represent the mapping of the current forwarding class into a new forwarding class, to be written into the header.

You define markers in the rewrite rules section of the class-of-service (CoS) configuration hierarchy and reference them in the logical interface configuration. You can configure different rewrite rules to handle VPN traffic and non-VPN traffic. The rewrite rule can be applied to MPLS and IPv4 packet headers simultaneously, making it possible to initialize MPLS experimental (EXP) and IP precedence bits at LSP ingress.

For a detailed example of how to configure rewrite rules for MPLS and IPv4 packets and for more information about how to configure statements at the **[edit class-of-service]** hierarchy level, see the *Class of Service Feature Guide for Routing Devices*.



## CHAPTER 8

# Pinging VPNs

- [Pinging VPNs, VPLS, and Layer 2 Circuits on page 115](#)
- [Setting the Forwarding Class of the Ping Packets on page 116](#)
- [Pinging a VPLS Routing Instance on page 116](#)
- [Pinging a Layer 2 VPN on page 116](#)
- [Pinging a Layer 3 VPN on page 117](#)
- [Pinging a Layer 2 Circuit on page 117](#)

### Pinging VPNs, VPLS, and Layer 2 Circuits

For testing purposes, you can ping Layer 2 VPNs, Layer 3 VPNs, and Layer 2 circuits by using the **ping mpls** command. The **ping mpls** command helps to verify that a VPN or circuit has been enabled and tests the integrity of the VPN or Layer 2 circuit connection between the PE routers. It does not test the connection between a PE router and a CE router. To ping a VPLS routing instance, you issue a **ping vpls instance** command (see [“Pinging a VPLS Routing Instance” on page 116](#)).

You issue the **ping mpls** command from the ingress PE router of the VPN or Layer 2 circuit to the egress PE router of the same VPN or Layer 2 circuit. When you execute the **ping mpls** command, echo requests are sent as MPLS packets.

The payload is a User Datagram Protocol (UDP) packet forwarded to the address **127.0.0.1**. The contents of this packet are defined in RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*. The label and interface information for building and sending this information as an MPLS packet is the same as for standard VPN traffic, but the time-to-live (TTL) of the innermost label is set to 1.

When the echo request arrives at the egress PE router, the contents of the packet are checked, and then a reply that contains the correct return is sent by means of UDP. The PE router sending the echo request waits to receive an echo reply after a timeout of 2 seconds (you cannot configure this value).

You must configure MPLS at the **[edit protocols mpls]** hierarchy level on the egress PE router (the router receiving the MPLS echo packets) to be able to ping the VPN or Layer 2 circuit. You must also configure the address **127.0.0.1/32** on the egress PE router's **lo0** interface. If this is not configured, the egress PE router does not have this forwarding entry and therefore simply drops the incoming MPLS pings.

The **ping mpls** command has the following limitations:

- You cannot ping an IPv6 destination prefix.
- You cannot ping a VPN or Layer 2 circuit from a router that is attempting a graceful restart.
- You cannot ping a VPN or Layer 2 circuit from a logical system.

You can also determine whether an LSP linking two PE routers in a VPN is up by pinging the end point address of the LSP. The command you use to ping an MPLS LSP end point is **ping mpls lsp-end-point address**. This command tells you what type of LSP (RSVP or LDP) terminates at the address specified and whether that LSP is up or down.

For a detailed description of this command, see the *Junos Routing Protocols and Policies Command Reference*.

---

## Setting the Forwarding Class of the Ping Packets

When you execute the **ping mpls** command, the ping packets forwarded to the destination include MPLS labels. It is possible to set the value of the forwarding class for these ping packets by using the **exp** option with the **ping mpls** command. For example, to set the forwarding class to 5 when pinging a Layer 3 VPN, issue the following command:

```
ping mpls l3vpn westcoast source 192.0.2.1 prefix 192.0.2.2 exp 5 count 20 detail
```

This command would make the router attempt to ping the Layer 3 VPN **westcoast** using ping packets with an EXP forwarding class of 5. The default forwarding class used for the **ping mpls** command packets is 7.

---

## Pinging a VPLS Routing Instance

The **ping vpls instance** command uses a difference command structure and operates in a different fashion than the **ping mpls** command used for VPNs and Layer 2 circuits. The **ping vpls instance** command is only supported on MX Series routers, the M120 router, the M320 router, and the T1600 router.

To ping a VPLS routing instance, use the following command:

```
ping vpls instance instance-name destination-mac address source-ip address <count
number> <data-plane-response> <detail> <learning-vlan-id number> <logical-system
logical-system-name>
```

You ping a combination of the routing instance name, the destination MAC address, and the source IP address. When you enter this command, you are provided feedback on the status of your request. An exclamation point (!) indicates that an echo reply was received. A period (.) indicates that an echo reply was not received within the timeout period. An x indicates that an echo reply was received with an error code these packets are not counted in the received packets count. They are accounted for separately.

---

## Pinging a Layer 2 VPN

To ping a Layer 2 VPN, use one of the following commands:



- **ping mpls l2vpn interface *interface-name***

You ping an interface configured for the Layer 2 VPN on the egress PE router.

- **ping mpls l2vpn instance *l2vpn-instance-name* local-site-id *local-site-id-number* remote-site-id *remote-site-id-number***

You ping a combination of the Layer 2 VPN routing instance name, the local site identifier, and the remote site identifier to test the integrity of the Layer 2 VPN connection (specified by the identifiers) between the ingress and egress PE routers.

#### Related Documentation

- [Example: Configuring MPLS-Based Layer 2 VPNs on page 148](#)

---

## Pinging a Layer 3 VPN

To ping a Layer 3 VPN, use the following command:

```
ping mpls l3vpn l3vpn-name prefix prefix <count count>
```

You ping a combination of an IPv4 destination prefix and a Layer 3 VPN name on the egress PE router to test the integrity of the VPN connection between the ingress and egress PE routers. The destination prefix corresponds to a prefix in the Layer 3 VPN. However, the ping tests only whether the prefix is present in a PE router's VRF table. It does not test the connection between a PE router and a CE router.

---

## Pinging a Layer 2 Circuit

To ping a Layer 2 circuit, use one of the following commands:

- **ping mpls l2circuit interface *interface-name***

You ping an interface configured for the Layer 2 circuit on the egress PE router.

- **ping mpls l2circuit virtual-circuit neighbor <*prefix*> <*virtual-circuit-id*>**

You ping a combination of the IPv4 prefix and the virtual circuit identifier on the egress PE router to test the integrity of the Layer 2 circuit between the ingress and egress PE routers.



## PART 2

# Common Configuration for Layer 2 VPNs and VPLS

- [Overview on page 121](#)
- [Layer 2 VPNs Configuration Overview on page 125](#)
- [Configuring Layer 2 Interfaces on page 163](#)
- [Configuring Path Selection for Layer 2 VPNs and VPLS on page 169](#)
- [Creating Backup Connections with Redundant Pseudowires on page 177](#)
- [Configuring Class of Service for Layer 2 VPNs on page 183](#)
- [Monitoring Layer 2 VPNs Using BFD on page 185](#)



## CHAPTER 9

# Overview

- [Understanding Layer 2 VPNs on page 121](#)
- [Layer 2 VPN Applications on page 122](#)
- [Supported Layer 2 VPN Standards on page 123](#)

### Understanding Layer 2 VPNs

---

As the need to link different Layer 2 services to one another for expanded service offerings grows, Layer 2 Multiprotocol Label Switching (MPLS) VPN services are increasingly in demand.

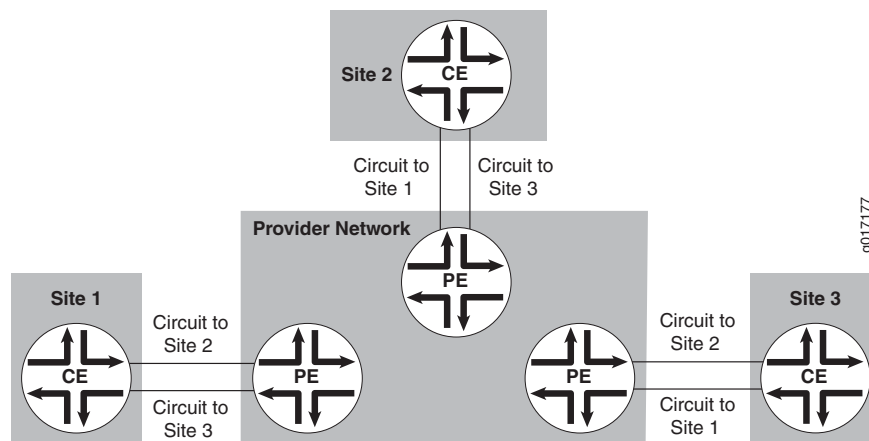
Implementing a Layer 2 VPN on a router is similar to implementing a VPN using a Layer 2 technology such as Asynchronous Transfer Mode (ATM) or Frame Relay. However, for a Layer 2 VPN on a router, traffic is forwarded to the router in a Layer 2 format. It is carried by MPLS over the service provider's network, and then converted back to Layer 2 format at the receiving site. You can configure different Layer 2 formats at the sending and receiving sites. The security and privacy of an MPLS Layer 2 VPN are equal to those of an ATM or Frame Relay VPN. The service provisioned with Layer 2 VPNs is also known as Virtual Private Wire Service (VPWS).

On a Layer 2 VPN, routing occurs on the customer's routers, typically on the customer edge (CE) router. The CE router connected to a service provider on a Layer 2 VPN must select the appropriate circuit on which to send traffic. The provider edge (PE) router receiving the traffic sends it across the service provider's network to the PE router connected to the receiving site. The PE routers do not need to store or process the customer's routes; they only need to be configured to send data to the appropriate tunnel.

For a Layer 2 VPN, customers need to configure their own routers to carry all Layer 3 traffic. The service provider needs to know only how much traffic the Layer 2 VPN will need to carry. The service provider's routers carry traffic between the customer's sites using Layer 2 VPN interfaces. The VPN topology is determined by policies configured on the PE routers.

Customers need to know only which VPN interfaces connect to which of their own sites. [Figure 9 on page 122](#) illustrates a Layer 2 VPN in which each site has a VPN interface linked to each of the other customer sites.

Figure 9: Layer 2 VPN Connecting CE Routers



Implementing a Layer 2 MPLS VPN includes the following benefits:

- Service providers do not have to invest in separate Layer 2 equipment to provide Layer 2 VPN service. A Layer 2 MPLS VPN allows you to provide Layer 2 VPN service over an existing IP and MPLS backbone.
- You can configure the PE router to run any Layer 3 protocol in addition to the Layer 2 protocols.
- Customers who prefer to maintain control over most of the administration of their own networks might want Layer 2 VPN connections with their service provider instead of a Layer 3 VPN.
- Because Layer 2 VPNs use BGP as the signaling protocol, they have a simpler design and require less overhead than traditional VPNs over Layer 2 circuits. BGP signaling also enables autodiscovery of Layer 2 VPN peers. Layer 2 VPNs are similar to BGP or MPLS VPNs and VPLS in many respects; all three types of services employ BGP for signaling.

## Layer 2 VPN Applications

Implementing a Layer 2 VPN includes the following benefits:

- Terminating a Layer 2 VPN into a Layer 2 VPN using the interworking (iw0) software interface eliminates the limitation of bandwidth on the tunnel interfaces used for these configuration scenarios. Instead of using a physical Tunnel PIC for looping the packet received from the Layer 2 VPN to another Layer 2 VPN, Junos OS is used to link both the Layer 2 VPN routes.
- Layer 2 VPNs enable the sharing of a provider's core network infrastructure between IP and Layer 2 VPN services, reducing the cost of providing those services. A Layer 2 MPLS VPN allows you to provide Layer 2 VPN service over an existing IP and MPLS backbone.

- From a service provider's point of view, a Layer 2 MPLS VPN allows the use of a single Layer 3 VPN (such as RFC 2547bis), MPLS traffic engineering, and Differentiated Services (DiffServ).
- Service providers do not have to invest in separate Layer 2 equipment to provide Layer 2 VPN service. You can configure the PE router to run any Layer 3 protocol in addition to the Layer 2 protocols. Customers who prefer to maintain control over most of the administration of their own networks might want Layer 2 VPN connections with their service provider instead of a Layer 3 VPN.

**Related  
Documentation**

- [Understanding Layer 2 VPNs on page 121](#)
- [Using the Layer 2 Interworking Interface to Interconnect a Layer 2 Circuit to a Layer 2 VPN on page 989](#)
- [Using the Layer 2 Interworking Interface to Interconnect a Layer 2 VPN to a Layer 2 VPN on page 945](#)
- [Example: Interconnecting a Layer 2 Circuit with a Layer 2 VPN on page 991](#)
- [Example: Interconnecting a Layer 2 VPN with a Layer 2 VPN on page 947](#)
- [Example: Interconnecting a Layer 2 VPN with a Layer 3 VPN on page 964](#)

## Supported Layer 2 VPN Standards

Junos OS substantially supports the following Internet drafts, which define standards for Layer 2 virtual private networks (VPNs).

- Internet draft draft-kompella-l2vpn-vpls-multihoming, *Multi-homing in BGP-based Virtual Private LAN Service*
- Internet draft draft-kompella-ppvpn-l2vpn-03.txt, *Layer 2 VPNs Over Tunnels*

**Related  
Documentation**

- [Supported Carrier-of-Carriers and Interprovider VPN Standards](#)
- [Supported VPWS Standards on page 450](#)
- [Supported Layer 3 VPN Standards](#)
- [Supported Multicast VPN Standards](#)
- [Supported VPLS Standards on page 542](#)
- [Accessing Standards Documents on the Internet](#)





# Layer 2 VPNs Configuration Overview

- [Introduction to Configuring Layer 2 VPNs on page 125](#)
- [Configuring the Local Site on PE Routers in Layer 2 VPNs on page 126](#)
- [Layer 2 VPN Configuration Example on page 132](#)
- [Example: Configuring MPLS-Based Layer 2 VPNs on page 148](#)
- [Transmitting Nonstandard BPDUs in Layer 2 VPNs and VPLS on page 162](#)

## Introduction to Configuring Layer 2 VPNs

---

To configure Layer 2 virtual private network (VPN) functionality, you must enable Layer 2 VPN support on the provider edge (PE) router. You must also configure PE routers to distribute routing information to the other PE routers in the VPN and configure the circuits between the PE routers and the customer edge (CE) routers.

Each Layer 2 VPN is configured under a routing instance of type **l2vpn**. An **l2vpn** routing instance can transparently carry Layer 3 traffic across the service provider's network. As with other routing instances, all logical interfaces belonging to a Layer 2 VPN routing instance are listed under that instance.

The configuration of the CE routers is not relevant to the service provider. The CE routers need to provide only appropriate Layer 2 circuits (with appropriate circuit identifiers, such as data-link connection identifier [DLCI], virtual path identifier/virtual channel identifier [VPI/VCI], or virtual LAN [VLAN] ID) to send traffic to the PE router.

To configure Layer 2 VPNs, include the following statements:

```
description text;
instance-type l2vpn;
interface interface-name;
route-distinguisher (as-number:id|ip-address:id);
vrf-export [policy-names];
vrf-import [policy-names];
vrf-target {
 community;
 import community-name;
 export community-name;
}
protocols {
 l2vpn {
```

```
(control-word | no-control-word);
encapsulation-type type;
site site-name {
 interface interface-name {
 description text;
 remote-site-id remote-site-id;
 }
 site-identifier identifier;
 site-preference preference-value {
 backup;
 primary;
 }
}
traceoptions {
 file filename <files number> <size size> <world-readable | no-world-readable>;
 flag flag <flag-modifier> <disable>;
}
}
```

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 2 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*.

In addition to these statements, you must configure MPLS label-switched paths (LSPs) between the PE routers, IBGP sessions between the PE routers, and an interior gateway protocol (IGP) on the PE and provider (P) routers. You must also configure the statements that are required for all types of VPN configuration.

By default, Layer 2 VPNs are disabled.

Many of the configuration procedures for Layer 2 VPNs are identical to the procedures for Layer 3 VPNs and virtual private LAN service (VPLS).

---

## Configuring the Local Site on PE Routers in Layer 2 VPNs

For each local site, the PE router advertises a set of VPN labels to the other PE routers servicing the Layer 2 VPN. The VPN labels constitute a single block of contiguous labels; however, to allow for reprovisioning, more than one such block can be advertised. Each label block consists of a label base, a range (the size of the block), and a remote site ID that identifies the sequence of remote sites that connect to the local site using this label block (the remote site ID is the first site identifier in the sequence). The encapsulation type is also advertised along with the label block.

The following sections explain how to configure the connections to the local site on the PE router:

- [Configuring a Layer 2 VPN Routing Instance on page 127](#)
- [Configuring the Site on page 127](#)

- [Configuring the Remote Site ID on page 128](#)
- [Configuring the Encapsulation Type on page 129](#)
- [Configuring a Site Preference and Layer 2 VPN Multihoming on page 130](#)
- [Tracing Layer 2 VPN Traffic and Operations on page 131](#)

## Configuring a Layer 2 VPN Routing Instance

To configure a Layer 2 VPN on your network, configure a Layer 2 VPN routing instance on the PE router by including the **l2vpn** statement:

```
l2vpn {
 (control-word | no-control-word);
 encapsulation-type type;
 traceoptions {
 file filename <files number> <size size> <world-readable | no-world-readable>;
 flag flag <flag-modifier> <disable>;
 }
 site site-name {
 site-identifier identifier;
 site-preference preference-value {
 backup;
 primary;
 }
 interface interface-name {
 description text;
 remote-site-id remote-site-id;
 }
 }
}
```

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]



**NOTE:** You cannot configure a routing protocol (OSPF, RIP, IS-IS or BGP) inside a Layer 2 VPN routing instance (instance-type **l2vpn**). The Junos CLI disallows this configuration.

Instructions for how to configure the remaining statements are included in the sections that follow.

## Configuring the Site

All the Layer 2 circuits provisioned for a local site are listed as the set of logical interfaces (specified by including the **interface** statement) within the **site** statement.

On each PE router, you must configure each site that has a circuit to the PE router. To do this, include the **site** statement:

```

site site-name {
 site-identifier identifier;
 site-preference preference-value {
 backup;
 primary;
 }
 interface interface-name {
 description text;
 remote-site-id remote-site-ID;
 }
}

```

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols l2vpn]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols l2vpn]

You must configure the following for each site:

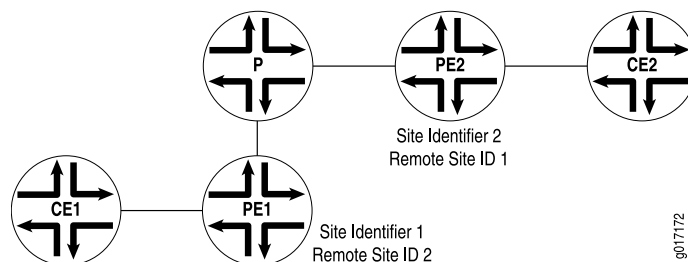
- **site-name**—Name of the site.
- **site-identifier *identifier***—Unsigned 16-bit number greater than zero that uniquely identifies the local Layer 2 VPN site. The site identifier corresponds to the remote site ID configured on another site within the same VPN.
- **interface *interface-name***—The name of the interface and, optionally, a remote site ID for remote site connections. See “[Configuring the Remote Site ID](#)” on page 128.

## Configuring the Remote Site ID

The remote site ID allows you to configure a sparse Layer 2 VPN topology. A sparse topology means that each site does not have to connect to all the other sites in the VPN; thus it is unnecessary to allocate circuits for all the remote sites. Remote site IDs are particularly important if you configure a topology more complicated than full-mesh, such as a hub-and-spoke topology.

The remote site ID (configured with the **remote-site-id** statement) corresponds to the site ID (configured with the **site-identifier** statement) configured at a separate site. [Figure 10 on page 128](#) illustrates the relationship between the site identifier and the remote site ID.

**Figure 10: Relationship Between the Site Identifier and the Remote Site ID**



As illustrated by the figure, the configuration for Router PE1 connected to Router CE1 is as follows:

```
site-identifier 1;
interface so-0/0/0 {
 remote-site-id 2;
}
```

The configuration for Router PE2 connected to Router CE2 is as follows:

```
site-identifier 2;
interface so-0/0/1 {
 remote-site-id 1;
}
```

The remote site ID (2) on Router PE1 corresponds to the site identifier (2) on Router PE2. On Router PE2, the remote site ID (1) corresponds to the site identifier (1) on Router PE1.

To configure the remote site ID, include the **remote-site-id** statement:

```
remote-site-id remote-site-id;
```

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols l2vpn site *site-name* interface *interface-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols l2vpn site *site-name* interface *interface-name*]

If you do not explicitly include the **remote-site-id** statement for the interface configured at the [edit routing-instances *routing-instance-name* protocols l2vpn site *site-name*] hierarchy level, a remote site ID is assigned to that interface.

The remote site ID for an interface is automatically set to 1 higher than the remote site ID for the previous interface. The order of the interfaces is based on their **site-identifier** statements. For example, if the first interface in the list does not have a remote site ID, its ID is set to 1. The second interface in the list has its remote site ID set to 2, and the third has its remote site ID set to 3. The remote site IDs of any interfaces that follow are incremented in the same manner if you do not explicitly configure them.

## Configuring the Encapsulation Type

The encapsulation type you configure at each Layer 2 VPN site varies depending on which Layer 2 protocol you choose to configure. If you configure **ethernet-vlan** as the encapsulation type, you need to use the same protocol at each Layer 2 VPN site.

You do not need to use the same protocol at each Layer 2 VPN site if you configure any of the following encapsulation types:

- **atm-aal5**—Asynchronous Transfer Mode (ATM) Adaptation Layer (AAL5)
- **atm-cell**—ATM cell relay
- **atm-cell-port-mode**—ATM cell relay port promiscuous mode

- **atm-cell-vc-mode**—ATM virtual circuit (VC) cell relay nonpromiscuous mode
- **atm-cell-vp-mode**—ATM virtual path (VP) cell relay promiscuous mode
- **cisco-hdlc**—Cisco Systems-compatible High-Level Data Link Control (HDLC)
- **ethernet**—Ethernet
- **ethernet-vlan**—Ethernet virtual LAN (VLAN)
- **frame-relay**—Frame Relay
- **frame-relay-port-mode**—Frame Relay port mode
- **interworking**—Layer 2.5 interworking VPN
- **ppp**—Point-to-Point Protocol (PPP)

If you configure different protocols at your Layer 2 VPN sites, you need to configure a translational cross-connect (TCC) encapsulation type. For more information, see [“Configuring TCC Encapsulation for Layer 2 VPNs and Layer 2 Circuits” on page 164](#).

To configure the Layer 2 protocol accepted by the PE router, specify the encapsulation type by including the **encapsulation-type** statement:

**encapsulation-type** *type*;

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols l2vpn]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols l2vpn]

## Configuring a Site Preference and Layer 2 VPN Multihoming

You can specify the preference value advertised for a particular Layer 2 VPN site. The site preference value is encoded in the BGP local preference attribute. When a PE router receives multiple advertisements with the same CE device identifier, the advertisement with the highest local preference value is preferred.

You can also use the **site-preference** statement to enable multihoming for Layer 2 VPNs. Multihoming allows you to connect a CE device to multiple PE routers. In the event that a connection to the primary PE router fails, traffic can be automatically switched to the backup PE router.

To configure a site preference for a Layer 2 VPN, include the **site-preference** statement:

```
site-preference preference-value {
 backup;
 primary;
}
```

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols l2vpn site *site-name*]

- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols l2vpn site *site-name*]

You can also specify either the **backup** option or the **primary** option for the **site-preference** statement. The backup option specifies the preference value as 1, the lowest possible value, ensuring that the Layer 2 VPN site is the least likely to be selected. The primary option specifies the preference value as 65,535, the highest possible value, ensuring that the Layer 2 VPN site is the most likely to be selected.

For Layer 2 VPN multihoming configurations, specifying the **primary** option for a Layer 2 VPN site designates the connection from the PE router to the CE device as the preferred connection if the CE device is also connected to another PE router. Specifying the **backup** option for a Layer 2 VPN site designates the connection from the PE router to the CE device as the secondary connection if the CE device is also connected to another PE router.

## Tracing Layer 2 VPN Traffic and Operations

To trace Layer 2 VPN protocol traffic, specify options for the **traceoptions** statement in the Layer 2 VPN configuration:

```
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 l2vpn]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols l2vpn]

The following trace flags display the operations associated with Layer 2 VPNs:

- **all**—All Layer 2 VPN tracing options.
- **connections**—Layer 2 connections (events and state changes).
- **error**—Error conditions.
- **general**—General events.
- **nlri**—Layer 2 advertisements received or sent by means of the BGP.
- **normal**—Normal events.
- **policy**—Policy processing.
- **route**—Routing information.
- **state**—State transitions.
- **task**—Routing protocol task processing.

- **timer**—Routing protocol timer processing.
- **topology**—Layer 2 VPN topology changes caused by reconfiguration or advertisements received from other PE routers using BGP.

---

### Disabling Normal TTL Decrementing for VPNs

To diagnose networking problems related to VPNs, it can be useful to disable normal time-to-live (TTL) decrementing. In Junos, you can do this with the **no-propagate-ttl** and **no-decrement-ttl** statements. However, when you are tracing VPN traffic, only the **no-propagate-ttl** statement is effective.

For the **no-propagate-ttl** statement to have an effect on VPN behavior, you need to clear the PE-router-to-PE-router BGP session, or disable and then enable the VPN routing instance.

For more information about the **no-propagate-ttl** and **no-decrement-ttl** statements, see the *Junos OS MPLS Applications Library for Routing Devices*.

---

## Layer 2 VPN Configuration Example

The following sections explain how to configure Layer 2 VPN functionality on the provider edge (PE) routers connected to each site:

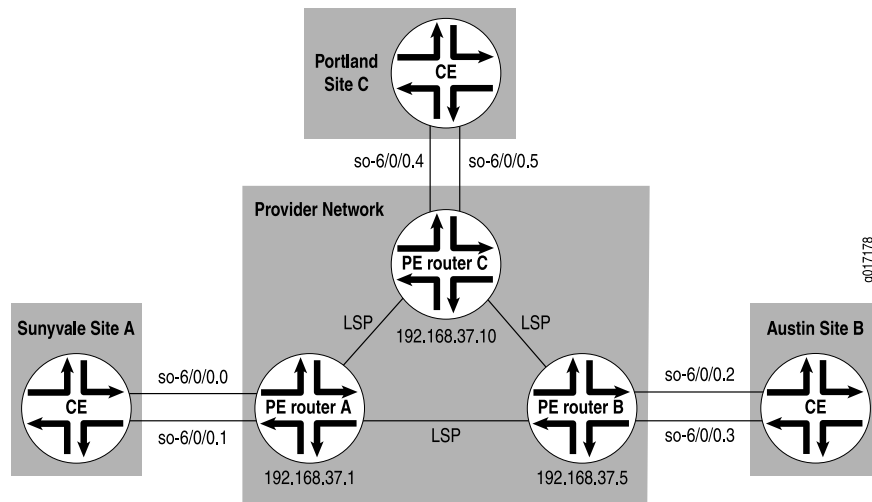
- [Simple Full-Mesh Layer 2 VPN Overview on page 132](#)
- [Enabling an IGP on the PE Routers on page 133](#)
- [Configuring MPLS LSP Tunnels Between the PE Routers on page 133](#)
- [Configuring IBGP on the PE Routers on page 134](#)
- [Configuring Routing Instances for Layer 2 VPNs on the PE Routers on page 136](#)
- [Configuring CCC Encapsulation on the Interfaces on page 138](#)
- [Configuring VPN Policy on the PE Routers on page 139](#)
- [Layer 2 VPN Configuration Summarized by Router on page 142](#)

### Simple Full-Mesh Layer 2 VPN Overview

In the sections that follow, you configure a simple full-mesh Layer 2 VPN spanning three sites: Sunnyvale, Austin, and Portland. Each site connects to a PE router. The customer edge (CE) routers at each site use Frame Relay to carry Layer 2 traffic to the PE routers. Since this example uses a full-mesh topology between all three sites, each site requires two logical interfaces (one for each of the other CE routers), although only one physical link is needed to connect each PE router to each CE router. [Figure 11 on page 133](#) illustrates the topology of this Layer 2 VPN.



Figure 11: Example of a Simple Full-Mesh Layer 2 VPN Topology



### Enabling an IGP on the PE Routers

To allow the PE routers to exchange routing information among themselves, you must configure an interior gateway protocol (IGP) or static routes on these routers. You configure the IGP on the master instance of the routing protocol process (rpd) (that is, at the **[edit protocols]** hierarchy level), not within the Layer 2 VPN routing instance (that is, not at the **[edit routing-instances]** hierarchy level). Turn on traffic engineering on the IGP.

You configure the IGP in the standard way. This example does not include this portion of the configuration.

### Configuring MPLS LSP Tunnels Between the PE Routers

In this configuration example, RSVP is used for MPLS signaling. Therefore, in addition to configuring RSVP, you must create an MPLS label-switched path (LSP) to tunnel the VPN traffic.

On Router A, enable RSVP and configure one end of the MPLS LSP tunnel to Router B. When configuring the MPLS LSP, include all interfaces using the **interface all** statement.

```
[edit]
protocols {
 rsvp {
 interface all;
 }
 mpls {
 interface all;
 label-switched-path RouterA-to-RouterB {
 to 192.168.37.5;
 primary Path-to-RouterB;
 }
 label-switched-path RouterA-to-RouterC {
 to 192.168.37.10;
 primary Path-to-RouterC;
 }
 }
}
```

```
 }
 }
}
```

On Router B, enable RSVP and configure the other end of the MPLS LSP tunnel. Again, configure the interfaces by using the **interface all** statement.

```
[edit]
protocols {
 rsvp {
 interface all;
 }
 mpls {
 interface all;
 label-switched-path RouterB-to-RouterA {
 to 192.168.37.1;
 primary Path-to-RouterA;
 }
 label-switched-path RouterB-to-RouterC {
 to 192.168.37.10;
 primary Path-to-RouterC;
 }
 }
}
```

On Router C, enable RSVP and configure the other end of the MPLS LSP tunnel. Again, configure all interfaces using the **interface all** statement.

```
[edit]
protocols {
 rsvp {
 interface all;
 }
 mpls {
 interface all;
 label-switched-path RouterC-to-RouterA {
 to 192.168.37.1;
 primary Path-to-RouterA;
 }
 label-switched-path RouterC-to-RouterB {
 to 192.168.37.5;
 primary Path-to-RouterB;
 }
 }
}
```

## Configuring IBGP on the PE Routers

On the PE routers, configure an IBGP session with the following parameters:

- Layer 2 VPN—To indicate that the IBGP session is for a Layer 2 VPN, include the **family l2vpn** statement.
- Local address—The IP address in the **local-address** statement is the same as the address configured in the **to** statement at the **[edit protocols mpls label-switched-path**

*lsp-path-name*] hierarchy level on the remote PE router. The IBGP session for Layer 2 VPNs runs through this address.

- Neighbor address—Include the **neighbor** statement, specifying the IP address of the neighboring PE router.

On Router A, configure IBGP:

```
[edit]
protocols {
 bgp {
 import match-all;
 export match-all;
 group pe-pe {
 type internal;
 neighbor 192.168.37.5 {
 local-address 192.168.37.1;
 family l2vpn {
 signaling;
 }
 }
 neighbor 192.168.37.10 {
 local-address 192.168.37.1;
 family l2vpn {
 signaling;
 }
 }
 }
 }
}
```

On Router B, configure IBGP:

```
[edit]
protocols {
 bgp {
 local-address 192.168.37.5;
 import match-all;
 export match-all;
 group pe-pe {
 type internal;
 neighbor 192.168.37.1 {
 local-address 192.168.37.5;
 family l2vpn {
 signaling;
 }
 }
 neighbor 192.168.37.10 {
 local-address 192.168.37.5;
 family l2vpn {
 signaling;
 }
 }
 }
 }
}
```

On Router C, configure IBGP:

```
[edit]
protocols {
 bgp {
 local-address 192.168.37.10;
 import match-all;
 export match-all;
 group pe-pe {
 type internal;
 neighbor 192.168.37.1 {
 local-address 192.168.37.10;
 family l2vpn {
 signaling;
 }
 }
 }
 neighbor 192.168.37.5 {
 local-address 192.168.37.10;
 family l2vpn {
 signaling;
 }
 }
 }
}
```

## Configuring Routing Instances for Layer 2 VPNs on the PE Routers

The three PE routers service the Layer 2 VPN, so you need to configure a routing instance on each router. For the VPN, you must define the following in each routing instance:

- Route distinguisher, which must be unique for each routing instance on the PE router. It is used to distinguish the addresses in one VPN from those in another VPN.
- Instance type of **l2vpn**, which configures the router to run a Layer 2 VPN.
- Interfaces connected to the CE routers.
- Virtual routing and forwarding (VRF) import and export policies, which must be the same on each PE router that services the same VPN and are used to control the network topology. Unless the import policy contains only a **then reject** statement, it must include a reference to a community. Otherwise, when you attempt to commit the configuration, the commit operation fails.

On Router A, configure the following routing instance for the Layer 2 VPN:

```
[edit]
routing-instances {
 VPN-Sunnyvale-Portland-Austin {
 instance-type l2vpn;
 interface so-6/0/0.0;
 interface so-6/0/0.1;
 route-distinguisher 100:1;
 vrf-import vpn-SPA-import;
 vrf-export vpn-SPA-export;
 protocols {
```

```

l2vpn {
 encapsulation-type frame-relay;
 site Sunnyvale {
 site-identifier 1;
 interface so-6/0/0.0 {
 remote-site-id 2;
 }
 interface so-6/0/0.1 {
 remote-site-id 3;
 }
 }
}

```

On Router B, configure the following routing instance for the Layer 2 VPN:

```

[edit]
routing-instances {
 VPN-Sunnyvale-Portland-Austin {
 instance-type l2vpn;
 interface so-6/0/0.2;
 interface so-6/0/0.3;
 route-distinguisher 100:1;
 vrf-import vpn-SPA-import;
 vrf-export vpn-SPA-export;
 protocols {
 l2vpn {
 encapsulation-type frame-relay;
 site Austin {
 site-identifier 2;
 interface so-6/0/0.2 {
 remote-site-id 1;
 }
 interface so-6/0/0.3 {
 remote-site-id 3;
 }
 }
 }
 }
 }
}

```

On Router C, configure the following routing instance for the Layer 2 VPN:

```

[edit]
routing-instances {
 VPN-Sunnyvale-Portland-Austin {
 instance-type l2vpn;
 interface so-6/0/0.4;
 interface so-6/0/0.5;
 route-distinguisher 100:1;
 vrf-import vpn-SPA-import;
 vrf-export vpn-SPA-export;
 protocols {
 l2vpn {

```

```
encapsulation-type frame-relay;
site Portland {
 site-identifier 3;
 interface so-6/0/0.4 {
 remote-site-id 1;
 }
 interface so-6/0/0.5 {
 remote-site-id 2;
 }
}
}
```

## Configuring CCC Encapsulation on the Interfaces

You need to specify a circuit cross-connect (CCC) encapsulation type for each PE-router-to-CE-router interface running in the Layer 2 VPN. This encapsulation type should match the encapsulation type configured under the routing instance.

Configure the following CCC encapsulation types for the interfaces on Router A:

```
[edit]
interfaces so-6/0/0 {
 encapsulation frame-relay-ccc;
 unit 0 {
 encapsulation frame-relay-ccc;
 }
}
interfaces so-6/0/0 {
 encapsulation frame-relay-ccc;
 unit 1 {
 encapsulation frame-relay-ccc;
 }
}
```

Configure the following CCC encapsulation types for the interfaces on Router B:

```
[edit]
interfaces so-6/0/0 {
 encapsulation frame-relay-ccc;
 unit 2 {
 encapsulation frame-relay-ccc;
 }
}
interfaces so-6/0/0 {
 encapsulation frame-relay-ccc;
 unit 3 {
 encapsulation frame-relay-ccc;
 }
}
```

Configure the following CCC encapsulation types for the interfaces on Router C:

```
[edit]
interface so-6/0/0 {
```

```

encapsulation frame-relay-ccc;
unit 4 {
 encapsulation frame-relay-ccc;
}
}
interface so-6/0/0 {
 encapsulation frame-relay-ccc;
 unit 5 {
 encapsulation frame-relay-ccc;
 }
}
}

```

## Configuring VPN Policy on the PE Routers

You must configure VPN import and export policies on each of the PE routers so that they install the appropriate routes in their VRF tables, which the routers use to forward packets within the VPN.



**NOTE:** Use the `community add community-name` statement at the `[edit policy-options policy-statement policy-statement-name term term-name then]` hierarchy level to facilitate Layer 2 VPN VRF export policies.

On Router A, configure the following VPN import and export policies:

```

[edit]
policy-options {
 policy-statement match-all {
 term acceptable {
 then accept;
 }
 }
 policy-statement vpn-SPA-export {
 term a {
 then {
 community add SPA-com;
 accept;
 }
 }
 term b {
 then reject;
 }
 }
 policy-statement vpn-SPA-import {
 term a {
 from {
 protocol bgp;
 community SPA-com;
 }
 then accept;
 }
 term b {
 then reject;
 }
 }
}

```

```
 }
 community SPA-com members target:69:100;
 }
```

On Router B, configure the following VPN import and export policies:

```
[edit]
policy-options {
 policy-statement match-all {
 term acceptable {
 then accept;
 }
 }
 policy-statement vpn-SPA-import {
 term a {
 from {
 protocol bgp;
 community SPA-com;
 }
 then accept;
 }
 term b {
 then reject;
 }
 }
 policy-statement vpn-SPA-export {
 term a {
 then {
 community add SPA-com;
 accept;
 }
 }
 term b {
 then reject;
 }
 }
 community SPA-com members target:69:100;
}
```

On Router C, configure the following VPN import and export policies:

```
[edit]
policy-options {
 policy-statement match-all {
 term acceptable {
 then accept;
 }
 }
 policy-statement vpn-SPA-import {
 term a {
 from {
 protocol bgp;
 community SPA-com;
 }
 then accept;
 }
 term b {
```



```

 then reject;
 }
}
policy-statement vpn-SPA-export {
 term a {
 then {
 community add SPA-com;
 accept;
 }
 }
 term b {
 then reject;
 }
}
community SPA-com members target:69:100;
}

```

To apply the VPN policies on the routers, include the **vrf-export** and **vrf-import** statements when you configure the routing instance. The VRF import and export policies handle the route distribution across the IBGP session running between the PE routers.

To apply the VPN policies on Router A, include the following statements:

```

[edit]
routing-instances {
 VPN-Sunnyvale-Portland-Austin {
 vrf-import vpn-SPA-import;
 vrf-export vpn-SPA-export;
 }
}

```

To apply the VPN policies on Router B, include the following statements:

```

[edit]
routing-instances {
 VPN-Sunnyvale-Portland-Austin {
 vrf-import vpn-SPA-import;
 vrf-export vpn-SPA-export;
 }
}

```

To apply the VPN policies on Router C, include the following statements:

```

[edit]
routing-instances {
 VPN-Sunnyvale-Portland-Austin {
 vrf-import vpn-SPA-import;
 vrf-export vpn-SPA-export;
 }
}

```

## Layer 2 VPN Configuration Summarized by Router

For a summary of the configuration on each router in the examples in this chapter, see the following sections:

- [Summary for Router A \(PE Router for Sunnyvale\) on page 142](#)
- [Summary for Router B \(PE Router for Austin\) on page 144](#)
- [Summary for Router C \(PE Router for Portland\) on page 146](#)

### Summary for Router A (PE Router for Sunnyvale)

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Routing Instance for<br>Layer 2 VPN                    | <pre>[edit] routing-instances {   VPN-Sunnyvale-Portland-Austin {     instance-type l2vpn;     interface so-6/0/0.0;     interface so-6/0/0.1;     route-distinguisher 100:1;     vrf-import vpn-SPA-import;     vrf-export vpn-SPA-export;     protocols {       l2vpn {         encapsulation-type frame-relay;         site Sunnyvale {           site-identifier 1;           interface so-6/0/0.0 {             remote-site-id 2;           }           interface so-6/0/0.1 {             remote-site-id 3;           }         }       }     }   } }</pre> |
| Configure CCC<br>Encapsulation Types<br>for Interfaces | <pre>interfaces {   interface so-6/0/0 {     encapsulation frame-relay-ccc;     unit 0 {       encapsulation frame-relay-ccc;     }   }   interface so-6/0/0 {     encapsulation frame-relay-ccc;     unit 1 {       encapsulation frame-relay-ccc;     }   } }</pre>                                                                                                                                                                                                                                                                                             |

|                                 |                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Master Protocol Instance</b> | <pre> protocols { } </pre>                                                                                                                                                                                                                                                                                                                     |
| <b>Enable RSVP</b>              | <pre> rsvp {   interface all; } </pre>                                                                                                                                                                                                                                                                                                         |
| <b>Configure MPLS LSPs</b>      | <pre> mpls {   label-switched-path RouterA-to-RouterB {     to 192.168.37.5;     primary Path-to-RouterB {       cspf;     }   }   label-switched-path RouterA-to-RouterC {     to 192.168.37.10;     primary Path-to-RouterC {       cspf;     }   } } interface all; } </pre>                                                                |
| <b>Configure IBGP</b>           | <pre> bgp {   import match-all;   export match-all;   group pe-pe {     type internal;     neighbor 192.168.37.5 {       local-address 192.168.37.1;       family l2vpn {         signaling;       }     }     neighbor 192.168.37.10 {       local-address 192.168.37.1;       family l2vpn {         signaling;       }     }   } } } </pre> |
| <b>Configure VPN Policy</b>     | <pre> policy-options {   policy-statement match-all {     term acceptable {       then accept;     }   } } policy-statement vpn-SPA-export {   term a {     then {       community add SPA-com;       accept;     }   } } </pre>                                                                                                               |

```
 }
 term b {
 then reject;
 }
}
policy-statement vpn-SPA-import {
 term a {
 from {
 protocol bgp;
 community SPA-com;
 }
 then accept;
 }
 term b {
 then reject;
 }
}
community SPA-com members target:69:100;
}
```

---

#### Summary for Router B (PE Router for Austin)

---

|                                                        |                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Routing Instance for<br>VPN                            | <pre>[edit]<br/>routing-instances {<br/>    VPN-Sunnyvale-Portland-Austin {<br/>        instance-type l2vpn;<br/>        interface so-6/0/0.2;<br/>        interface so-6/0/0.3;<br/>        route-distinguisher 100:1;<br/>        vrf-import vpn-SPA-import;<br/>        vrf-export vpn-SPA-export;<br/>    }<br/>}</pre>                                                 |
| Configure Layer 2 VPN                                  | <pre>protocols {<br/>    l2vpn {<br/>        encapsulation-type frame-relay;<br/>        site Austin {<br/>            site-identifier 2;<br/>            interface so-6/0/0.2 {<br/>                remote-site-id 1;<br/>            }<br/>            interface so-6/0/0.3 {<br/>                remote-site-id 3;<br/>            }<br/>        }<br/>    }<br/>}</pre> |
| Configure CCC<br>Encapsulation Types<br>for Interfaces | <pre>[edit]<br/>interfaces {<br/>    interface so-6/0/0 {<br/>        encapsulation frame-relay-ccc;<br/>        unit 2 {<br/>            encapsulation frame-relay-ccc;<br/>        }<br/>    }<br/>}</pre>                                                                                                                                                                |

```

 }
 }
 interface so-6/0/0 {
 encapsulation frame-relay-ccc;
 unit 3 {
 encapsulation frame-relay-ccc;
 }
 }
}

Master Protocol Instance protocols {
}

Enable RSVP rsvp {
 interface all;
}

Configure MPLS LSPs mpls {
 label-switched-path RouterB-to-RouterA {
 to 192.168.37.1;
 primary Path-to-RouterA {
 cspf;
 }
 }
 label-switched-path RouterB-to-RouterC {
 to 192.168.37.10;
 primary Path-to-RouterC {
 cspf;
 }
 }
 interface all;
}

Configure IBGP bgp {
 local-address 192.168.37.5;
 import match-all;
 export match-all;
 group pe-pe {
 type internal;
 neighbor 192.168.37.1 {
 local-address 192.168.37.5;
 family l2vpn {
 signaling;
 }
 }
 neighbor 192.168.37.10 {
 local-address 192.168.37.5;
 family l2vpn {
 signaling;
 }
 }
 }
}

Configure VPN Policy policy-options {

```

```
policy-statement match-all {
 term acceptable {
 then accept;
 }
}
policy-statement vpn-SPA-import {
 term a {
 from {
 protocol bgp;
 community SPA-com;
 }
 then accept;
 }
 term b {
 then reject;
 }
}
policy-statement vpn-SPA-export {
 term a {
 then {
 community add SPA-com;
 accept;
 }
 }
 term b {
 then reject;
 }
}
community SPA-com members target:69:100;
}
```

---

#### Summary for Router C (PE Router for Portland)

---

|                          |                                                                                                                                                                                                                                                             |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Routing Instance for VPN | <pre>[edit] routing-instances {   VPN-Sunnyvale-Portland-Austin {     instance-type l2vpn;     interface so-6/0/0.3;     interface so-6/0/0.4;     route-distinguisher 100:1;     vrf-import vpn-SPA-import;     vrf-export vpn-SPA-export;   } }</pre>     |
| Configure Layer 2 VPN    | <pre>protocols {   l2vpn {     encapsulation-type frame-relay;     site Portland {       site-identifier 3;       interface so-6/0/0.4 {         remote-site-id 1;       }       interface so-6/0/0.5 {         remote-site-id 2;       }     }   } }</pre> |

|                                                  |                                                                                                                                                                                                                                                                                |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                  | <pre>         }       }     }   } </pre>                                                                                                                                                                                                                                       |
| Configure CCC Encapsulation Types for Interfaces | <pre> [edit] interfaces {   interface so-6/0/0 {     encapsulation frame-relay-ccc;     unit 4 {       encapsulation frame-relay-ccc;     }   }   interface so-6/0/0 {     encapsulation frame-relay-ccc;     unit 5 {       encapsulation frame-relay-ccc;     }   } } </pre> |
| Master Protocol Instance                         | <pre> protocols { } </pre>                                                                                                                                                                                                                                                     |
| Enable RSVP                                      | <pre> rsvp {   interface all; } </pre>                                                                                                                                                                                                                                         |
| Configure MPLS LSPs                              | <pre> mpls {   label-switched-path RouterC-to-RouterA {     to 192.168.37.1;     primary Path-to-RouterA {       cspf;     }   }   label-switched-path RouterC-to-RouterB {     to 192.168.37.5;     primary Path-to-RouterB {       cspf;     }   }   interface all; } </pre> |
| Configure IBGP                                   | <pre> bgp {   local-address 192.168.37.10;   import match-all;   export match-all;   group pe-pe {     type internal;     neighbor 192.168.37.1 {       local-address 192.168.37.10;       family l2vpn {         signaling;       }     }   } } </pre>                        |

```
 }
 neighbor 192.168.37.5 {
 local-address 192.168.37.10;
 family l2vpn {
 signaling;
 }
 }
}
```

**Configure VPN Policy**

```
policy-options {
 policy-statement match-all {
 term acceptable {
 then accept;
 }
 }
 policy-statement vpn-SPA-import {
 term a {
 from {
 protocol bgp;
 community SPA-com;
 }
 then accept;
 }
 term b {
 then reject;
 }
 }
 policy-statement vpn-SPA-export {
 term a {
 then {
 community add SPA-com;
 accept;
 }
 }
 term b {
 then reject;
 }
 }
 community SPA-com members target:69:100;
}
```

---

**Example: Configuring MPLS-Based Layer 2 VPNs**

---

You can implement an MPLS-based Layer 2 virtual private network (VPN) using Junos OS routing devices to interconnect customer sites with Layer 2 technology. Layer 2 VPNs give customers complete control of their own routing. To support an MPLS-based Layer 2 VPN, you need to add components to the configuration of the two provider edge (PE) routing devices. You do not need to change the configuration of the provider devices.

This example shows how to configure an MPLS-based Layer 2 VPN.





**NOTE:** You can configure both an MPLS-based Layer 2 VPN and an MPLS-based Layer 3 VPN on the same device. However, you cannot configure the same customer edge interface to support both a Layer 2 VPN and a Layer 3 VPN. The core interfaces and the loopback interfaces are configured in the same way for Layer 2 VPNs and Layer 3 VPNs.

- [Requirements on page 149](#)
- [Overview and Topology on page 149](#)
- [Configuring the Local PE Routing Device on page 152](#)
- [Configuring the Remote PE Routing Device on page 155](#)
- [Verification on page 158](#)

## Requirements

This example uses the following hardware and software components:

- Junos OS Release 11.1 or later if you are using EX Series switches
- Two PE routing devices

Before you configure the Layer 2 VPN components, configure the basic components for an MPLS network:

- Configure two PE routing devices. See *Configuring MPLS on Provider Edge EX8200 and EX4500 Switches Using Circuit Cross-Connect (CLI Procedure)*.
- Configure one or more provider devices. See *Configuring MPLS on EX8200 and EX4500 Provider Switches (CLI Procedure)*.



**NOTE:** A Layer 2 VPN requires that the PE routing devices be configured using circuit cross-connect (CCC). The provider routing devices are configured in the same way for MPLS using CCC and for IP over MPLS.

## Overview and Topology

A Layer 2 VPN provides complete separation between the provider's network and the customer's network—that is, the PE devices and the CE devices do not exchange routing information. Some benefits of a Layer 2 VPN are that it is private, secure, and flexible.

This example shows how to configure Layer 2 VPN components on the local and remote PE devices. This example does not include configuring a provider device, because there are no specific Layer 2 VPN components on the provider devices.

In the basic MPLS configuration of the PE devices using a circuit cross-connect (CCC), the PE devices are configured to use an interior gateway protocol (IGP), such as OSPF or IS-IS, as the routing protocol between the MPLS devices and LDP or RSVP as the signaling protocol. Traffic engineering is enabled. A label-switched path (LSP) is

configured within the **[edit protocols]** hierarchy. However, unlike the basic MPLS configuration using a CCC, you do not need to associate the LSP with the customer edge interface. When you are configuring a Layer 2 VPN, you must use BGP signaling. The BGP signaling automates the connections, so manual configuration of the association between the LSP and the customer edge interface is not required.

The following components must be added to the PE routing devices for an MPLS-based Layer 2 VPN:

- BGP group with **family l2vpn signaling**
- Routing instance using instance type **l2vpn**
- The physical layer encapsulation type (**ethernet**) must be specified on the customer edge interface and the encapsulation type must also be specified in the configuration of the routing instance.

Figure 12 on page 150 illustrates the topology of this MPLS-based Layer 2 VPN.

Figure 12: MPLS-Based Layer 2 VPN

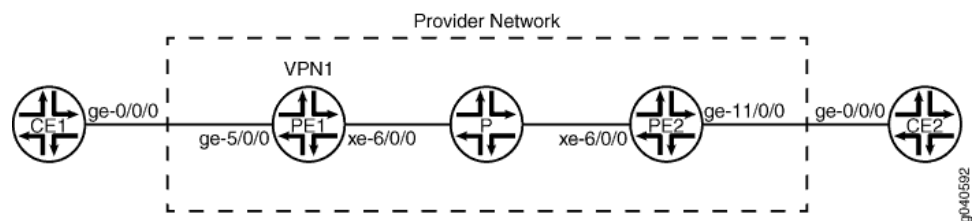


Table 3 on page 150 shows the settings of the customer edge interface on the local CE device.

Table 3: Local CE Routing Device in the MPLS-Based Layer 2 VPN Topology

| Property                         | Settings                                                                    | Description                         |
|----------------------------------|-----------------------------------------------------------------------------|-------------------------------------|
| Local CE routing device hardware | Routing device                                                              | CE1                                 |
| Customer edge interface          | <b>ge-0/0/0 unit 0</b><br><b>family inet</b><br><b>address 192.0.2.2/24</b> | Interface that connects CE1 to PE1. |

Table 4 on page 150 shows the settings of the customer edge interface on the remote CE routing device.

Table 4: Remote CE Routing Device in the MPLS-Based Layer 2 VPN Topology

| Property                          | Settings                                                                    | Description                         |
|-----------------------------------|-----------------------------------------------------------------------------|-------------------------------------|
| Remote CE routing device hardware | Routing device                                                              | CE2                                 |
| Customer edge interface           | <b>ge-0/0/0 unit 0</b><br><b>family inet</b><br><b>address 192.0.2.1/24</b> | Interface that connects CE2 to PE2. |

Table 5 on page 151 shows the Layer 2 VPN components of the local PE routing device.

**Table 5: Layer 2 VPN Components of the Local PE Routing Device**

| Property                         | Settings                                                                                                                        | Description                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Local PE routing device hardware | Routing device                                                                                                                  | PE1                                                                                                                                                                                                                                                                                                                                                                             |
| Customer edge interface          | <b>ge-5/0/0</b><br><b>encapsulation ethernet-ccc</b><br><b>unit 0</b><br><b>family ccc</b>                                      | Connects PE1 to CE1.<br><br>For the Layer 2 VPN, add <b>ethernet-ccc</b> as the physical layer encapsulation type.<br><br><b>NOTE:</b> The <b>family ccc</b> should already have been completed as part of the basic MPLS configuration of a PE routing device for circuit cross-connect. It is included here to show what was specified for that portion of the configuration. |
| Core interface                   | <b>xe-6/0/0 unit 0</b><br><b>family inet address 192.0.2.6/24</b><br><b>family iso</b><br><b>family mpls</b>                    | Connects PE1 to P.<br><br><b>NOTE:</b> This portion of the configuration should already have been completed as part of the basic MPLS configuration. It is included here to show what was specified for that portion of the configuration.                                                                                                                                      |
| Loopback interface               | <b>lo0 unit 0</b><br><b>family inet address 203.0.113.1/24</b><br><b>family iso address</b><br><b>49.0001.2102.2021.0210.00</b> | <b>NOTE:</b> This portion of the configuration should already have been completed as part of the basic MPLS configuration. It is included here to show what was specified for that portion of the configuration.                                                                                                                                                                |
| BGP                              | <b>bgp</b>                                                                                                                      | Added for the Layer 2 VPN configuration.                                                                                                                                                                                                                                                                                                                                        |
| Routing instance                 | <b>vpn1</b>                                                                                                                     | Added for the Layer 2 VPN configuration                                                                                                                                                                                                                                                                                                                                         |

Table 6 on page 151 shows the Layer 2 VPN components of the remote PE routing device.

**Table 6: Layer 2 VPN Components of the Remote PE Routing Device**

| Property                   | Settings       | Description |
|----------------------------|----------------|-------------|
| PE routing device hardware | Routing device | PE2         |

Table 6: Layer 2 VPN Components of the Remote PE Routing Device (*continued*)

| Property                | Settings                                                                                                                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Customer edge interface | <code>ge-11/0/0</code><br><code>encapsulation ethernet-ccc</code><br><code>unit 0</code><br><code>family ccc</code>                                                                     | Connects PE2 to CE2.<br><br>For the Layer 2 VPN, add <b>ethernet-ccc</b> as the physical layer encapsulation type.<br><br><b>NOTE:</b> The <b>family ccc</b> should already have been completed as part of the basic MPLS configuration of a PE routing device for circuit cross-connect. It is included here to show what was specified for that portion of the configuration. |
| Core interface          | <code>xe-6/0/0</code><br><br><code>unit 0</code><br><code>family inet</code><br><code>address 192.0.2.7/24</code><br><code>family iso</code><br><code>family mpls</code>                | Connects PE2 to P.<br><br><b>NOTE:</b> This portion of the configuration should already have been completed as part of the basic MPLS configuration. It is included here to show what was specified for that portion of the configuration.                                                                                                                                      |
| Loopback interface      | <code>lo0</code><br><code>unit 0</code><br><code>family inet</code><br><code>address 203.0.113.2/24</code><br><code>family iso</code><br><code>address 49.0001.2202.2022.0220.00</code> | <b>NOTE:</b> This portion of the configuration should already have been completed as part of the basic MPLS configuration. It is included here to show what was specified for that portion of the configuration.                                                                                                                                                                |
| BGP                     | <code>bgp</code>                                                                                                                                                                        | Added for the Layer 2 VPN configuration.                                                                                                                                                                                                                                                                                                                                        |
| Routing instance        | <code>vpn1</code>                                                                                                                                                                       | Added for the Layer 2 VPN configuration.                                                                                                                                                                                                                                                                                                                                        |

## Configuring the Local PE Routing Device

**CLI Quick Configuration** To quickly configure the Layer 2 VPN components on the local PE routing device, copy the following commands and paste them into the routing device terminal window:

```
[edit]
set interfaces ge-5/0/0 encapsulation ethernet-ccc
set protocols bgp group ibgp local-address 203.0.113.1 family l2vpn signaling
set protocols bgp group ibgp type internal
set protocols bgp group ibgp neighbor 203.0.113.2
set routing-instances vpn1 instance-type l2vpn
set routing-instances vpn1 interface ge-5/0/0
set routing-instances vpn1 route-distinguisher 203.0.113.1:21
set routing-instances vpn1 vrf-target target:21:21
set routing-instances vpn1 protocols l2vpn encapsulation-type ethernet
set routing-instances vpn1 protocols l2vpn interface ge-5/0/0.0 description "BETWEEN PE1 AND CE1"
set routing-instances vpn1 protocols l2vpn site JE-V21 site-identifier 21 interface ge-5/0/0
remote-site-id 26
```

**Step-by-Step Procedure**

To configure the Layer 2 VPN components on the local PE routing device:

1. Configure the customer edge interface to use the physical encapsulation type **ethernet-ccc**:  

```
[edit]
user@PE1# set interfaces ge-5/0/0 encapsulation ethernet-ccc
```
2. Configure BGP, specifying the loopback address as the local address and enabling **family l2vpn signaling**:  

```
[edit protocols bgp]
user@PE1# set group ibgp local-address 203.0.113.1 family l2vpn signaling
```
3. Configure the BGP group, specifying the group name and type:  

```
[edit protocols bgp]
user@PE1# set group ibgp type internal
```
4. Configure the BGP neighbor, specifying the loopback address of the remote PE routing device as the neighbor's address:  

```
[edit protocols bgp]
user@PE1# set group ibgp neighbor 203.0.113.2
```
5. Configure the routing instance, specifying the routing-instance name and using **l2vpn** as the instance type:  

```
[edit routing-instances]
user@PE1# set vpn1 instance-type l2vpn
```
6. Configure the routing instance to apply to the customer edge interface:  

```
[edit routing-instances]
user@PE1# set vpn1 interface ge-5/0/0
```
7. Configure the routing instance to use a route distinguisher:  

```
[edit routing-instances]
user@PE1# set vpn1 route-distinguisher 203.0.113.1:21
```
8. Configure the VPN routing and forwarding (VRF) target of the routing instance:  

```
[edit routing-instances]
user@PE1# set vpn1 vrf-target target:21:21
```



**NOTE:** You can create more complex policies by explicitly configuring VRF import and export policies using the import and export options. See the [Junos OS VPNs Configuration Guide](#).

9. Configure the protocols and encapsulation type used by the routing instance:  

```
[edit routing-instances]
user@PE1# set vpn1 protocols l2vpn encapsulation-type ethernet
```
10. Apply the routing instance to a customer edge interface and specify a description for it:  

```
[edit routing-instances]
user@PE1# set vpn1 protocols interface ge-5/0/0.0 description "BETWEEN PE1 AND CE1"
```
11. Configure the routing-instance protocols site:  

```
[edit routing-instances]
user@PE1# set vpn1 protocols l2vpn site JE-V21 site-identifier 21 remote-site-id 26
```



**NOTE:** The remote site ID (configured with the `remote-site-id` statement) corresponds to the site ID (configured with the `site-identifier` statement) configured on the other PE routing device.

**Results** Display the results of the configuration:

```
user@PE1# show

interfaces {
 ge-5/0/0 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
 }
 xe-6/0/0 {
 unit 0 {
 family inet {
 address 192.0.2.6/24;
 }
 family mpls;
 }
 }
 lo0 {
 unit 0 {
 family inet {
 address 203.0.113.1/24;
 }
 family iso {
 address 49.0001.2102.2021.0210.00;
 }
 }
 }
}

protocols {
 rsvp {
 interface lo0.0;
 interface xe-0/0/6.0;
 }
 mpls {
 label-switched-path lsp_to_pe2 {
 to 203.0.113.2;
 }
 interface xe-0/0/6.0;
 }
 bgp {
 group ibgp {
 type internal;
 local-address 203.0.113.1;
 family inet-vpn {
 signaling;
 }
 neighbor 203.0.113.2;
 }
 }
}
```

```

 }
 }
 routing-instances {
 vpn1 {
 instance-type l2vpn;
 interface ge-5/0/0.0;
 route-distinguisher 203.0.113.1:21;
 vrf-target target:21:21;
 protocols {
 l2vpn {
 encapsulation-type ethernet;
 interface ge-5/0/0.0 {
 description "BETWEEN PE1 AND CE1";
 }
 site JE-V21 {
 site-identifier 21;
 interface ge-5/0/0.0 {
 remote-site-id 26;
 }
 }
 }
 }
 }
 }
}

```

## Configuring the Remote PE Routing Device

**CLI Quick Configuration** To quickly configure the Layer 2 VPN components on the remote PE routing device, copy the following commands and paste them into the routing device terminal window:

```

[edit]
set interfaces ge-11/0/0 encapsulation ethernet-ccc
set protocols bgp group ibgp local-address 203.0.113.2 family l2vpn signaling
set protocols bgp group ibgp type internal
set protocols bgp group ibgp neighbor 203.0.113.1
set routing-instances vpn1 instance-type l2vpn
set routing-instances vpn1 interface ge-11/0/0
set routing-instances vpn1 route-distinguisher 203.0.113.1:21
set routing-instances vpn1 vrf-target target:21:21
set routing-instances vpn1 protocols l2vpn encapsulation-type ethernet
set routing-instances vpn1 protocols l2vpn interface ge-11/0/0.0 description "BETWEEN PE1 AND CE1"
set routing-instances vpn1 protocols l2vpn site T26-VPN1 site-identifier 26 remote-site-id 21

```

**Step-by-Step Procedure** To configure the Layer 2 VPN components on the remote PE routing device:

1. Configure the customer edge interface to use the physical encapsulation type **ethernet-ccc**:  

```

[edit]
user@PE1# set interfaces ge-11/0/0 encapsulation ethernet-ccc

```
2. Configure BGP, specifying the loopback address as the **local-address** and specifying **family l2vpn signaling**:  

```

[edit protocols bgp]
user@PE2# set group ibgp local-address 203.0.113.2 family l2vpn signaling

```
3. Configure the BGP group, specifying the group name and type:  

```

[edit protocols bgp]

```

- ```

user@PE2# set group ibgp type internal

```
4. Configure the BGP neighbor, specifying the loopback address of the remote PE routing device as the neighbor's address:


```

[edit protocols bgp]
user@PE2# set group ibgp neighbor 203.0.113.1

```
 5. Configure the routing instance, specifying the routing-instance name and using **l2vpn** as the **instance-type**:


```

[edit routing-instances]
user@PE2# set vpn1 instance-type l2vpn

```
 6. Configure the routing instance to apply to the customer edge interface:


```

[edit routing-instances]
user@PE2# set vpn1 interface ge-11/0/0.0

```
 7. Configure the routing instance to use a route distinguisher, using the format *ip-address:number*:


```

[edit routing-instances]
user@PE2# set vpn1 route-distinguisher 203.0.113.1:21

```
 8. Configure the VPN routing and forwarding (VRF) target of the routing instance:


```

[edit routing-instances]
user@PE2# set vpn1 vrf-target target:21:21

```
 9. Configure the protocols and encapsulation type used by the routing instance:


```

[edit routing-instances]
user@PE2# set vpn1 protocols l2vpn encapsulation-type ethernet

```
 10. Apply the routing instance to a customer edge interface and specify a description for it:


```

[edit routing-instances]
user@PE1# set vpn1 protocols interface ge-11/0/0.0 description "BETWEEN PE1 AND CE1"

```
 11. Configure the routing-instance protocols site:


```

[edit routing-instances]
user@PE2# set vpn1 protocols l2vpn site T26-VPN1 site-identifier 26 remote-site-id 21

```



NOTE: The remote site ID (configured with the `remote-site-id` statement) corresponds to the site ID (configured with the `site-identifier` statement) configured on the other PE routing device.

Results Display the results of the configuration:

```

user@PE2# show

interfaces {
  ge-11/0/0 {
    encapsulation ethernet-ccc;
    unit 0 {
      family ccc;
    }
  }
  xe-6/0/0 {
    unit 0 {
      family inet {

```



```

        address 192.0.2.7/24;
    }
    family mpls;
}
}
lo0 {
    unit 0 {
        family inet {
            address 203.0.113.2/24;
        }
        family iso {
            address 49.0001.2202.2022.0220.00;
        }
    }
}
protocols {
    rsvp {
        interface lo0.0;
        interface xe-0/0/6.0;
    }
    mpls {
        label-switched-path lsp_to_pe1 {
            to 203.0.113.1;
        }
    }
    interface xe-0/0/6.0;
    bgp {
        group ibgp
        type internal
        local-address 203.0.113.1
        family inet-vpn
        unicast
    }
}
routing-instances {
    vpn1 {
        instance-type l2vpn;
        interface ge-11/0/0.0;
        route-distinguisher 203.0.113.1:21;
        vrf-target target:21:21;
        protocols {
            l2vpn {
                encapsulation-type ethernet;
                interface ge-11/0/0.0 {
                    description "BETWEEN PE1 AND CE1";
                }
            }
            site T26-VPN1 {
                site-identifier 26;
                interface ge-11/0/0.0 {
                    remote-site-id 21;
                }
            }
        }
    }
}
}
}

```

Verification

To confirm that the MPLS-based Layer 2 VPN is working properly, perform these tasks:

- [Verifying the Layer 2 VPN Connection on page 158](#)
- [Verifying the Status of MPLS Label-Switched Paths on page 159](#)
- [Verifying BGP Status on page 159](#)
- [Verifying the Status of the RSVP Sessions on page 159](#)
- [Verifying the Routes in the Routing Table on page 160](#)
- [Pinging the Layer 2 VPN Connections on page 161](#)

Verifying the Layer 2 VPN Connection

Purpose Verify that the Layer 2 VPN connection is up.

Action user@PE1> [show l2vpn connections](#)

Layer-2 VPN connections:

Legend for connection status (St)

EI -- encapsulation invalid	NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch	WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down	NP -- interface hardware not present
CM -- control-word mismatch	-> -- only outbound connection is up
CN -- circuit not provisioned	<- -- only inbound connection is up
OR -- out of range	Up -- operational
OL -- no outgoing label	Dn -- down
LD -- local site signaled down	CF -- call admission control failure
RD -- remote site signaled down	SC -- local and remote site ID collision
LN -- local site not designated	LM -- local site ID not minimum designated
RN -- remote site not designated	RM -- remote site ID not minimum designated
XX -- unknown connection status	IL -- no incoming label
MM -- MTU mismatch	MI -- Mesh-Group ID not available
BK -- Backup connection	ST -- Standby connection
PF -- Profile parse failure	PB -- Profile busy
RS -- remote site standby	SN -- Static Neighbor

Legend for interface status

Up -- operational
Dn -- down

Instance: vpn1

Local site: JE-V21 (21)

connection-site	Type	St	Time last up	# Up trans
26	rmt	Up	Apr 16 05:53:21 2010	1

Remote PE: 203.0.113.2, Negotiated control-word: Yes (Null)
Incoming label: 800000, Outgoing label: 800001
Local interface: ge-5/0/0.0, Status: Up, Encapsulation: ETHERNET

Meaning The **St** field in the output shows that the Layer 2 VPN connection to **Remote PE (203.0.113.2)** is up.

Verifying the Status of MPLS Label-Switched Paths

Purpose Verify that the MPLS label-switched paths (ingress and egress) are up.

Action user@PE1> show mpls lsp

Ingress LSP: 1 sessions

To	From	State	Rt	P	ActivePath	LSPName
203.0.113.2	203.0.113.1	Up	0	*		lsp_to_pe2

Total 1 displayed, Up 1, Down 0

Egress LSP: 1 sessions

To	From	State	Rt	Style	Labelin	Labelout	LSPName
203.0.113.1	203.0.113.2	Up	0	1 FF	3	-	lsp_to_pe1

Total 1 displayed, Up 1, Down 0

Transit LSP: 0 sessions
Total 0 displayed, Up 0, Down 0

Meaning The **State** field in the output shows that the Ingress LSP to **Remote PE (203.0.113.2)** is up, and the Egress LSP from the remote PE routing device to this PE routing device (**203.0.113.1**) is also up.

Verifying BGP Status

Purpose Verify that BGP is up.

Action user@PE1> show bgp summary

Groups: 1 Peers: 1 Down peers: 0

Table	Tot Paths	Act Paths	Suppressed	History	Damp	State	Pending
bgp.l2vpn.0	1	1	0	0	0	0	0

Peer	AS	InPkt	OutPkt	OutQ	Flaps	Last	Up/Dwn
203.0.113.2	10	33	34	0	1	13:24	

State|#Active/Received/Accepted/Damped...

Establ

bgp.l2vpn.0: 1/1/1/0
vpn2.l2vpn.0: 1/1/1/0

Meaning The output shows that the remote PE routing device (**203.0.113.2**) is listed as the BGP peer and that a protocol session has been established. It also shows the number of packets received from the remote PE routing device (**33**) and the number of packets sent (**34**) to the remote PE routing device.

Verifying the Status of the RSVP Sessions

Purpose Verify that the RSVP sessions (ingress and egress) are up.

Action user@PE1> show rsvp session

Ingress RSVP: 1 sessions

To	From	State	Rt	Style	Labelin	Labelout	LSPname
203.0.113.2	203.0.113.1	Up	0	1 FF	-	462880	lsp_to_pe2

Total 1 displayed, Up 1, Down 0

Egress RSVP: 1 sessions

To	From	State	Rt	Style	Labelin	Labelout	LSPname
203.0.113.1	203.0.113.2	Up	0	1 FF	3	-	lsp_to_pe1

Total 1 displayed, Up 1, Down 0

Transit RSVP: 0 sessions

Total 0 displayed, Up 0, Down 0

Meaning The output shows that both the ingress RSVP session and the egress RSVP session are up.

Verifying the Routes in the Routing Table

Purpose On routing device PE 1, use the **show route table** command to verify that the routing table is populated with the Layer 2 VPN routes used to forward the traffic.

Action user@PE1> show route table bgp.l2vpn.0

```
bgp.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
```

```
2:2:27:27/96
    *[BGP/170] 00:13:55, localpref 100, from 203.0.113.2
    AS path: I
    > to 198.51.100.6 via ge-6/0/46.0, label-switched-path
lsp_to_pe2
```

user@PE1> show route table vpn1.l2vpn.0

```
vpn1.l2vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
```

```
2:2:27:27/96
    *[BGP/170] 00:14:00, localpref 100, from 203.0.113.2
    AS path: I
    > to 198.51.100.6 via ge-6/0/46.0, label-switched-path
lsp_to_pe2
2:2:28:27/96
    *[L2VPN/170/-101] 00:15:55, metric2 1
    Indirect
```

Meaning The command **show route table bgp.l2vpn.0** displays all Layer 2 VPN routes that have been created on this routing device. The command **show route table vpn1.l2vpn.0** shows the Layer 2 VPN routes that have been created for the routing instance **vpn1**.

Pinging the Layer 2 VPN Connections

Purpose Verify connectivity.

Action user@PE1> `ping mpls l2vpn interface xe-6/0/0.0 reply-mode ip-udp`
!!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss

user@PE1> `ping mpls l2vpn instance vpn1 remote-site-id 26 local-site-id 21 detail`
Request for seq 1, to interface 68, labels <800001, 100176>
Reply for seq 1, return code: Egress-ok
Request for seq 2, to interface 68, labels <800001, 100176>
Reply for seq 2, return code: Egress-ok
Request for seq 3, to interface 68, labels <800001, 100176>
Reply for seq 3, return code: Egress-ok
Request for seq 4, to interface 68, labels <800001, 100176>
Reply for seq 4, return code: Egress-ok
Request for seq 5, to interface 68, labels <800001, 100176>
Reply for seq 5, return code: Egress-ok

--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss

Meaning The output shows that connectivity is established.

- Related Documentation**
- *Example: Configuring MPLS on EX8200 and EX4500 Switches*
 - *Example: Configuring MPLS-Based Layer 3 VPNs on EX Series Switches*
 - *Configuring an MPLS-Based Layer 2 VPN (CLI Procedure)*

Transmitting Nonstandard BPDUs in Layer 2 VPNs and VPLS

Circuit cross-connect (CCC) protocol, Layer 2 circuit, and Layer 2 VPN configurations can transmit nonstandard bridge protocol data units (BPDUs) generated by other vendors' equipment. This is the default behavior on all supported PICs and requires no additional configuration.

The following PICs are supported on T Series Core Routers and the M320 Multiservice Edge router and can transmit nonstandard BPDUs:

- 1-port Gigabit Ethernet PIC
- 2-port Gigabit Ethernet PIC
- 4-port Gigabit Ethernet PIC
- 10-port Gigabit Ethernet PIC

Configuring Layer 2 Interfaces

- [Configuring CCC Encapsulation for Layer 2 VPNs on page 163](#)
- [Configuring TCC Encapsulation for Layer 2 VPNs and Layer 2 Circuits on page 164](#)
- [Configuring the MTU for Layer 2 Interfaces on page 165](#)
- [Disabling the Control Word for Layer 2 VPNs on page 167](#)

Configuring CCC Encapsulation for Layer 2 VPNs

You need to specify a circuit cross-connect (CCC) encapsulation type for each PE-router-to-CE-router interface running a Layer 2 VPN. This encapsulation type should match the encapsulation type configured under the routing instance. For information about how to configure the encapsulation type under the routing instance, see [“Configuring the Encapsulation Type” on page 129](#).



NOTE: A Layer 2 VPN or Layer 2 circuit is not supported if the PE-router-to-P-router interface has VLAN-tagging enabled and uses a nonenhanced Flexible PIC Concentrator (FPC).

For Layer 2 VPNs, you need to configure the CCC encapsulation on the logical interface. You also need to configure an encapsulation on the physical interface. The physical interface encapsulation does not have to be a CCC encapsulation. However, it should match the logical interface encapsulation. For example, if you configure an ATM CCC encapsulation type on the logical interface, you should configure a compatible ATM encapsulation on the physical interface.

To configure the CCC encapsulation type, include the **encapsulation-type** statement:

```
encapsulation-type ccc-encapsulation-type;
```

To configure the CCC encapsulation type on the physical interface, include this statement at the following hierarchy levels:

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

To configure the CCC encapsulation type on the logical interface, include this statement at the following hierarchy levels:

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

You configure the encapsulation type at the **[edit interfaces]** hierarchy level differently from the **[edit routing-instances]** hierarchy level. For example, you specify the encapsulation as **frame-relay** at the **[edit routing-instances]** hierarchy level and as **frame-relay-ccc** at the **[edit interfaces]** hierarchy level.

You can run both standard Frame Relay and CCC Frame Relay on the same device. If you specify Frame Relay encapsulation (**frame-relay-ccc**) for the interface, you should also configure the encapsulation at the **[edit interfaces *interface name* unit *unit-number*]** hierarchy level as **frame-relay-ccc**. Otherwise, the logical interface unit defaults to standard Frame Relay.

Configuring TCC Encapsulation for Layer 2 VPNs and Layer 2 Circuits

Also known as Layer 2.5 VPNs, the translation cross-connect (TCC) encapsulation types allow you to configure different encapsulation types at the ingress and egress of a Layer 2 VPN or the ingress and egress of a Layer 2 circuit. For example, a CE router at the ingress of a Layer 2 VPN path can send traffic in a Frame Relay encapsulation. A CE router at the egress of that path can receive the traffic in an ATM encapsulation.

For information about how to configure encapsulations for Layer 2 circuits, see [“Configuring the Interface Encapsulation Type for Layer 2 Circuits” on page 356](#).

The configuration for TCC encapsulation types is similar to the configuration for CCC encapsulation types. For Layer 2 VPNs, you specify a TCC encapsulation type for each PE-router-to-CE-router interface. The encapsulation type configured for the interface should match the encapsulation type configured under the routing instance. For information about how to configure the encapsulation type under the routing instance, see [“Configuring the Encapsulation Type” on page 129](#).



NOTE: Some platform and FPC combinations can not pass TCC encapsulated ISO traffic. See *Platforms/FPCs That Cannot Forward TCC Encapsulated ISO Traffic* for details.

You need to configure the TCC encapsulation on both the physical and logical interfaces. To configure the TCC encapsulation type, include the **encapsulation-type** statement:

encapsulation-type *tcc-encapsulation-type*;

To configure the TCC encapsulation type on the physical interface, include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name*]**

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

To configure the TCC encapsulation type on the logical interface, include this statement at the following hierarchy levels:

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

You configure the encapsulation type at the [edit interfaces] hierarchy level differently than at the [edit routing-instances] hierarchy level. For example, you specify the encapsulation as **frame-relay** at the [edit routing-instances] hierarchy level and as **frame-relay-tcc** at the [edit interfaces] hierarchy level.

For Layer 2.5 VPNs employing an Ethernet interface as the TCC router, you can configure an Ethernet TCC or an extended VLAN TCC.

To configure an Ethernet TCC or an extended VLAN TCC, include the **proxy** and **remote** statements:

```
proxy inet-address;
remote (inet-address | mac-address);
```

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family tcc]
- [edit logical-interfaces *logical-interface-name* interfaces *interface-name* unit *logical-unit-number* family tcc]

The **proxy inet-address** address statement defines the IP address for which the TCC router is acting as proxy.

The **remote (inet-address | mac-address)** statement defines the location of the remote router.

Ethernet TCC is supported on interfaces that carry IP version 4 (IPv4) traffic only. However, Ethernet TCC encapsulation is not supported on 8-port, 12-port, and 48-port Fast Ethernet PICs.

Configuring the MTU for Layer 2 Interfaces

By default, the MTU used to advertise a Layer 2 pseudowire is determined by taking the interface MTU for the associated physical interface and subtracting the encapsulation overhead for sending IP packets based on the encapsulation. However, encapsulations that support multiple logical interfaces (and multiple Layer 2 pseudowires) rely on the same interface MTU (since they are all associated with the same physical interface). This can prove to be a limitation for VLAN Layer 2 pseudowires using the same Ethernet interface or for Layer 2 pseudowire DLCIs using the same Frame Relay interface.

This can also affect multivendor environments. For example, if you have three PE devices supplied by different vendors and one of the devices only supports an MTU of 1500, even

if the other devices support larger MTUs you must configure the MTU as 1500 (the smallest MTU of the three PE devices).

You can explicitly configure which MTU is advertised for a Layer 2 pseudowire, even if the Layer 2 pseudowire is sharing a physical interface with other Layer pseudowires. When you explicitly configure an MTU for a Layer 2 pseudowire, be aware of the following:

- For BGP-based applications such as l2vpn and bgp-vpls, the advertised MTU will be zero unless an MTU value is explicitly set at the **[edit routing-instances routing-instance-name protocols (l2vpn | vpls) site site-name]** hierarchy level.
- An explicitly configured MTU is signaled to the remote PE device. The configured MTU is also compared to the MTU received from the remote PE device. If there is a conflict, the Layer 2 pseudowire is taken down.
- If you configure an MTU for an ATM cell relay interface on an ATM II PIC, the configured MTU is used to compute the cell bundle size advertised for that Layer 2 pseudowire, instead of the default interface MTU.
- A configured MTU is used only in the control plane. It is not enforced in the data plane. You need to ensure that the CE device for a given Layer 2 pseudowire uses the correct MTU for data transmission.

The following procedure describes how to configure the MTU for the Layer 2 interface. This information applies to the following Layer 2 technologies:

- Layer 2 VPNs
- Layer 2 Circuits
- VPLS

1. To configure the MTU for a Layer 2 circuit, include the **mtu** statement:

```
mtu mtu-number;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

2. To allow a Layer 2 pseudowire to be established even though the MTU configured on the local PE router does not match the MTU configured on the remote PE router, include the **ignore-mtu-mismatch** statement:

```
ignore-mtu-mismatch;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

**Related
Documentation**

- [ignore-mtu-mismatch on page 1119](#)
- [mtu on page 1152](#)

Disabling the Control Word for Layer 2 VPNs

A 4-byte control word provides support for the emulated VC encapsulation for Layer 2 VPNs. This control word is added between the Layer 2 protocol data unit (PDU) being transported and the VC label that is used for demultiplexing. Various networking formats (ATM, Frame Relay, Ethernet, and so on) use the control word in a variety of ways.

On networks with equipment that does not support the control word, you can disable it by including the **no-control-word** statement:

no-control-word;

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols l2vpn]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols l2vpn]

For more information about configuring the control word, see “[Configuring the Control Word for Layer 2 Circuits](#)” on page 351 and the *Layer 2 Circuits Feature Guide*.



NOTE: Use the **no-control-word** statement to disable the control word when the topology uses generic routing encapsulation (GRE) as the connection mechanism between PEs, and one of the PEs is an M Series router.

Related Documentation

- [Configuring the Control Word for Layer 2 Circuits on page 351](#)
- [control-word on page 1083](#)
- [l2vpn on page 1129](#)

Configuring Path Selection for Layer 2 VPNs and VPLS

- [Understanding BGP Path Selection on page 169](#)
- [Enabling BGP Path Selection for Layer 2 VPNs and VPLS on page 173](#)
- [VPLS Path Selection Process for PE Routers on page 175](#)

Understanding BGP Path Selection

For each prefix in the routing table, the routing protocol process selects a single best path. After the best path is selected, the route is installed in the routing table. The best path becomes the active route if the same prefix is not learned by a protocol with a lower (more preferred) global preference value, also known as the administrative distance. The algorithm for determining the active route is as follows:

1. Verify that the next hop can be resolved.
2. Choose the path with the lowest preference value (routing protocol process preference).

Routes that are not eligible to be used for forwarding (for example, because they were rejected by routing policy or because a next hop is inaccessible) have a preference of -1 and are never chosen.
3. Prefer the path with higher local preference.

For non-BGP paths, choose the path with the lowest **preference2** value.
4. If the accumulated interior gateway protocol (AIGP) attribute is enabled, prefer the path with the lower AIGP attribute.
5. Prefer the path with the shortest autonomous system (AS) path value (skipped if the **as-path-ignore** statement is configured).

A confederation segment (sequence or set) has a path length of 0. An AS set has a path length of 1.
6. Prefer the route with the lower origin code.

Routes learned from an IGP have a lower origin code than those learned from an exterior gateway protocol (EGP), and both have lower origin codes than incomplete routes (routes whose origin is unknown).

7. Prefer the path with the lowest multiple exit discriminator (MED) metric.

Depending on whether nondeterministic routing table path selection behavior is configured, there are two possible cases:

- If nondeterministic routing table path selection behavior is not configured (that is, if the **path-selection cisco-nondeterministic** statement is not included in the BGP configuration), for paths with the same neighboring AS numbers at the front of the AS path, prefer the path with the lowest MED metric. To always compare MEDs whether or not the peer ASs of the compared routes are the same, include the **path-selection always-compare-med** statement.
- If nondeterministic routing table path selection behavior is configured (that is, the **path-selection cisco-nondeterministic** statement is included in the BGP configuration), prefer the path with the lowest MED metric.

Confederations are not considered when determining neighboring ASs. A missing MED metric is treated as if a MED were present but zero.



NOTE: MED comparison works for single path selection within an AS (when the route does not include an AS path), though this usage is uncommon.

By default, only the MEDs of routes that have the same peer autonomous systems (ASs) are compared. You can configure routing table path selection options to obtain different behaviors.

8. Prefer strictly internal paths, which include IGP routes and locally generated routes (static, direct, local, and so forth).
9. Prefer strictly external BGP (EBGP) paths over external paths learned through internal BGP (IBGP) sessions.
10. Prefer the path whose next hop is resolved through the IGP route with the lowest metric.



NOTE: A path is considered a BGP equal-cost path (and will be used for forwarding) if a tie-break is performed after the previous step. All paths with the same neighboring AS, learned by a multipath-enabled BGP neighbor, are considered.

BGP multipath does not apply to paths that share the same MED-plus-IGP cost yet differ in IGP cost. Multipath path selection is based on the IGP cost metric, even if two paths have the same MED-plus-IGP cost.

11. If both paths are external, prefer the currently active path to minimize route-flapping. This rule is not used if any one of the following conditions is true:
 - **path-selection external-router-id** is configured.
 - Both peers have the same router ID.

- Either peer is a confederation peer.
 - Neither path is the current active path.
12. Prefer a primary route over a secondary route. A primary route is one that belongs to the routing table. A secondary route is one that is added to the routing table through an export policy.
 13. Prefer the path from the peer with the lowest router ID. For any path with an originator ID attribute, substitute the originator ID for the router ID during router ID comparison.
 14. Prefer the path with the shortest cluster list length. The length is 0 for no list.
 15. Prefer the path from the peer with the lowest peer IP address.

Routing Table Path Selection

The shortest AS path step of the algorithm, by default, evaluates the length of the AS path and determines the active path. You can configure an option that enables Junos OS to skip this step of the algorithm by including the **as-path-ignore** option.



NOTE: The **as-path-ignore** option is not supported for routing instances.

To configure routing table path selection behavior, include the **path-selection** statement:

```
path-selection {
  (always-compare-med | cisco-non-deterministic | external-router-id);
  as-path-ignore;
  med-plus-igp {
    igp-multiplier number;
    med-multiplier number;
  }
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Routing table path selection can be configured in one of the following ways:

- Emulate the Cisco IOS default behavior (**cisco-non-deterministic**). This mode evaluates routes in the order that they are received and does not group them according to their neighboring AS. With **cisco-non-deterministic** mode, the active path is always first. All inactive, but eligible, paths follow the active path and are maintained in the order in which they were received, with the most recent path first. Ineligible paths remain at the end of the list.

As an example, suppose you have three path advertisements for the 192.168.1.0 /24 route:

- Path 1—learned through EBGp; AS Path of 65010; MED of 200
- Path 2—learned through IBGP; AS Path of 65020; MED of 150; IGP cost of 5
- Path 3—learned through IBGP; AS Path of 65010; MED of 100; IGP cost of 10

These advertisements are received in quick succession, within a second, in the order listed. Path 3 is received most recently, so the routing device compares it against path 2, the next most recent advertisement. The cost to the IBGP peer is better for path 2, so the routing device eliminates path 3 from contention. When comparing paths 1 and 2, the routing device prefers path 1 because it is received from an EBGP peer. This allows the routing device to install path 1 as the active path for the route.



NOTE: We do not recommend using this configuration option in your network. It is provided solely for interoperability to allow all routing devices in the network to make consistent route selections.

- Always comparing MEDs whether or not the peer ASs of the compared routes are the same (**always-compare-med**).
- Override the rule that If both paths are external, the currently active path is preferred (**external-router-id**). Continue with the next step (Step 12) in the path-selection process.
- Adding the IGP cost to the next-hop destination to the MED value before comparing MED values for path selection (**med-plus-igp**).

BGP multipath does not apply to paths that share the same MED-plus-IGP cost, yet differ in IGP cost. Multipath path selection is based on the IGP cost metric, even if two paths have the same MED-plus-IGP cost.

Effects of Advertising Multiple Paths to a Destination

BGP advertises only the active path, unless you configure BGP to advertise multiple paths to a destination.

Suppose a routing device has in its routing table four paths to a destination and is configured to advertise up to three paths (**add-path send path-count 3**). The three paths are chosen based on path selection criteria. That is, the three best paths are chosen in path-selection order. The best path is the active path. This path is removed from consideration and a new best path is chosen. This process is repeated until the specified number of paths is reached.

Related Documentation

- *Example: Ignoring the AS Path Attribute When Selecting the Best Path*
- *Examples: Configuring BGP MED*
- *Example: Advertising Multiple BGP Paths to a Destination*

Enabling BGP Path Selection for Layer 2 VPNs and VPLS

Layer 2 VPNs and VPLS share the same path selection process for determining the optimal path to reach all of the destinations shared within a single routing instance. For Layer 2 VPN and VPLS topologies, the path selection process is straightforward if there is just a single path from each PE router to each CE device. However, the path selection process becomes more complex if the PE routers receive two or more valid paths to reach a specific CE device.



NOTE: In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

The following network scenarios provide examples of what might cause a PE router to receive more than one valid path to reach a specific CE device:

- **Multihoming**—One or more CE devices within a routing instance are multihomed to two or more PE routers. Each multihomed CE device has at least two valid paths.
- **Route reflectors**—There are multiple route reflectors deployed within the same network and they are supporting PE routers within the same routing instance. Due to time delays in large complex networks, the route reflectors can separately receive a different valid path to reach a CE device at different times. When they readvertise these valid paths, a PE router could receive two or more separate but apparently valid paths to the same CE device.

By default, Juniper Networks routers use just the designated forwarder path selection algorithm to select the best path to reach each Layer 2 VPN or VPLS routing instance destination (for more information, see [“VPLS Path Selection Process for PE Routers” on page 175](#)). However, you can also configure the routers in your network to use both the BGP path selection algorithm and the designated forwarder path selection algorithm as follows:

- On the Provider routers within the service providers network, the standard BGP path selection algorithm is used (for more information, see [“Understanding BGP Path Selection” on page 169](#)). Using the standard BGP path selection for Layer 2 VPN and VPLS routes allows a service provider to leverage the existing Layer 3 VPN network infrastructure to also support Layer 2 VPNs and VPLS. The BGP path selection algorithm also helps to ensure that the service provider’s network behaves predictably with regard to Layer 2 VPN and VPLS path selection. This is particularly important in networks employing route reflectors and multihoming.

When a Provider router receives multiple paths for the same destination prefix (for example, a multihomed CE device), one path is selected based on the BGP path selection algorithm and placed in the `bgp.l2vpn.0` routing table and the appropriate `instance.l2vpn.0` routing table.

- When a PE router receives all of the available paths to each CE device, it runs the designated forwarder path selection algorithm to select the preferred path to reach each CE device, independently of the results of the earlier BGP path selection algorithm run on the Provider router. The VPLS designated forwarder algorithm uses the D-bit, preference, and PE router identifier to determine which of the valid paths to each CE device to use. The PE router might select a path to reach a CE device which is different from the path selected by the BGP-based Provider routers. In this scenario, the following is the expected behavior for traffic sent to the multihomed CE device:
 - If the path selected by the remote PE router is available, traffic will traverse the network to the multihomed CE device using the remote PE router's preferred path (again, ignoring the path selected by the BGP-based Provider routers).
 - If the path selected by the remote PE router fails:
 1. The Provider routers switch the traffic destined for the multihomed CE device to the alternate path as soon as failure is detected.
 2. The Provider routers notify the remote PE routers of the path failure.
 3. The remote PE routers update their routing tables accordingly.

For more information about the VPLS designated forwarder path selection algorithm, see [“VPLS Path Selection Process for PE Routers” on page 175](#). This algorithm is also described in the Internet draft [draft-kompella-l2vpn-vpls-multihoming-03.txt](#), *Multi-homing in BGP-based Virtual Private LAN Service*.

To enable the BGP path selection algorithm for Layer 2 VPN and VPLS routing instances, complete the following steps:

1. Run Junos OS Release 12.3 or later on all of the PE and Provider routers participating in Layer 2 VPN or VPLS routing instances.

Attempting to enable this functionality on a network with a mix of routers that both do and do not support this feature can result in anomalous behavior.

2. Specify a unique route distinguisher on each PE router participating in a Layer 2 VPN or VPLS routing instance.
3. Configure the [l2vpn-use-bgp-rules](#) statement on all of the PE and Provider routers participating in Layer 2 VPN or VPLS routing instances.

You can configure this statement at the **[edit protocols bgp path-selection]** hierarchy level to apply this behavior to all of the routing instances on the router or at the **[edit routing-instances routing-instance-name protocols bgp path-selection]** hierarchy level to apply this behavior to a specific routing instance.

Related Documentation

- [Understanding BGP Path Selection on page 169](#)
- [VPLS Path Selection Process for PE Routers on page 175](#)
- [l2vpn-use-bgp-rules on page 1133](#)
- [route-distinguisher on page 1051](#)

VPLS Path Selection Process for PE Routers

The VPLS path selection process is used to select the best path between a remote PE router and a local PE router in a VPLS network. This path selection process is applied to routes received from both single-homed and multi-homed PE routers.



NOTE: In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

When the VPLS path selection process is complete, a PE router is made the designated VPLS edge (VE) device. The designated VE device effectively acts as the endpoint for the VPLS pseudowire that is signaled from the remote PE router. Once a PE router is made the designated VE device, a pseudowire can be signaled between the remote PE router and the local PE router and then VPLS packets can begin to flow between the PE routers.

Routes from multihomed PE routers connected to the same customer site share the same site ID, but can have different route distinguishers and block offsets. You can alter the configurations of the route distinguishers and block offsets to make a router more likely or less likely to be selected as the designated VE device.

On each PE router in the VPLS network, the best path to the CE device is determined by completing the following VPLS path selection process on each route advertisement received:

1. If the advertisement has the down bit set to 0, the advertisement is discarded.
2. Select the path with a higher preference. The preference attribute is obtained from the site-preference configured using the **site-preference** statement at the **[edit routing-instances routing-instance-name protocols vpls site site-name]** hierarchy level. If the site preference is 0, the preference attribute is obtained from the local preference.
3. If the preference values are the same, select the path with the lower router ID.
4. If the router IDs are the same, the routes are from the same PE router and the advertisement is considered to be an update. The router ID corresponds to the value of the originator ID for the BGP attribute (if present). Otherwise, the IP address for the remote BGP peer is used.
5. If the block offset values are the same, the advertisement is considered to be an update.

Once the VPLS path selection process has been completed and the designated VE device has been selected, a pseudowire is signaled between the remote PE router and the local PE router.



NOTE: The VPLS path selection process works the same whether or not the route has been received from another PE router, a route reflector, or an autonomous system border router (ASBR).

When the remote PE router establishes or refreshes a pseudowire to the local PE router, it verifies that the prefix is in the range required for the site ID based on the block offset and label range advertised by the designated VE device. If the prefix is out of range, the pseudowire status is set to out of range.

The following cases outline the potential decisions that could be made when a PE router completes the VPLS path selection process for a Layer 2 advertisement in the VPLS network:

- The PE router originated one of the advertisements and selected its own advertisement as the best path.

This PE router has been selected as the designated VE device. Selection as the designated VE device triggers the creation of pseudowires to and from the other PE routers in the VPLS network. If the remote customer site is multihomed, the designated VE device triggers the creation of pseudowires to and from only the designated VE device for the remote site.

- The PE router originated one of the advertisements but did not select its own advertisement as the best path.

This PE router is a redundant PE router for a multihomed site, but it was not selected as the designated VE device. However, if this PE router has just transitioned from being the designated VE device (meaning it was receiving traffic from the remote PE routers addressed to the multihomed customer site), the PE router tears down all the pseudowires that it had to and from the other PE routers in the VPLS network.

- The PE router received the route advertisements and selected a best path. It did not originate any of these advertisements because it was not connected to the customer site.

If the best path to the customer site (the designated VE device) has not changed, nothing happens. If the best path has changed, this PE router brings up pseudowires to and from the newly designated VE device and tears down the pseudowires to and from the previously designated VE device.

If this PE router does not select a best path after running the VPLS path selection process, then the local PE router does not consider the remote site to exist.

When a VE device receives an advertisement for a Layer 2 NLRI that matches its own site ID but the site is not multihomed, the pseudowire between the VE device and the transmitting PE router transitions to a site collision state and is not considered to be up.

**Related
Documentation**

- [BGP Route Reflectors for VPLS on page 552](#)

Creating Backup Connections with Redundant Pseudowires

- [Redundant Pseudowires for Layer 2 Circuits and VPLS on page 177](#)
- [Configuring Redundant Pseudowires for Layer 2 Circuits and VPLS on page 179](#)

Redundant Pseudowires for Layer 2 Circuits and VPLS

A redundant pseudowire can act as a backup connection between PE routers and CE devices, maintaining Layer 2 circuit and VPLS services after certain types of failures. This feature can help improve the reliability of certain types of networks (metro for example) where a single point of failure could interrupt service for multiple customers. Redundant pseudowires cannot reduce traffic loss to zero. However, they provide a way to gracefully recover from pseudowire failures in such a way that service can be restarted within a known time limit.



NOTE: VPLS is not supported on ACX Series routers.

When you configure redundant pseudowires to remote PE routers, you configure one to act as the primary pseudowire over which customer traffic is being transmitted and you configure another pseudowire to act as a backup in the event the primary fails. You configure the two pseudowires statically. A separate label is allocated for the primary and backup neighbors.

For information about how to configure redundant pseudowires, see [“Configuring Redundant Pseudowires for Layer 2 Circuits and VPLS” on page 179](#).

The following sections provide an overview of redundant pseudowires for Layer 2 circuits and VPLS:

- [Types of Redundant Pseudowire Configurations on page 178](#)
- [Pseudowire Failure Detection on page 179](#)

Types of Redundant Pseudowire Configurations

You can configure redundant pseudowires for Layer 2 circuits and VPLS in either of the following manners:



NOTE: VPLS is not supported on ACX Series routers.

- You can configure a single active pseudowire. The PE router configured as the primary neighbor is given preference and this connection is the one used for customer traffic. For the LDP signalling, labels are exchanged for both incoming and outgoing traffic with the primary neighbor. The LDP label advertisement is accepted from the backup neighbor, but no label advertisement is forwarded to it, leaving the pseudowire in an incomplete state. The pseudowire to the backup neighbor is completed only when the primary neighbor fails. The decision to switch between the two pseudowires is made by the device configured with the redundant pseudowires. The primary remote PE router is unaware of the redundant configuration, ensuring that traffic is always switched using just the active pseudowire.
- Alternatively, you can configure two active pseudowires, one to each of the PE routers. Using this approach, control plane signalling is completed and active pseudowires are established with both the primary and backup neighbors. However, the data plane forwarding is done only over a one of the pseudowires (designated as the active pseudowire by the local device). The other pseudowire is on standby. The active pseudowire is preferably established with the primary neighbor and can switch to the backup pseudowire if the primary fails.

The decision to switch between the active and standby pseudowires is controlled by the local device. The remote PE routers are unaware of the redundant connection, and so both remote PE routers send traffic to the local device. The local device only accepts traffic from the active pseudowire and drops the traffic from the standby. In addition, the local device only sends traffic to the active pseudowire. If the active pseudowire fails, traffic is immediately switched to the standby pseudowire.

The two configurations available for pseudowire redundancy have the following limitations:

- For the single active pseudowire configuration, it takes more time (compared to the two active pseudowire configuration) to switchover to the backup pseudowire when a failure is detected. This approach requires additional control plane signalling to complete the pseudowire with the backup neighbor and traffic can be lost during the switchover from primary to backup.
- If you configure two active pseudowires, bandwidth is lost on the link carrying the backup pseudowire between the remote PE router and the local device. Traffic is always duplicated over both the active and standby pseudowires. The single active pseudowire configuration does not waste bandwidth in this fashion.

Pseudowire Failure Detection

The following events are used to detect a failure (control and data plane) of the pseudowire configured between a local device and a remote PE router and initiates the switch to a redundant pseudowire:

- Manual switchover (user initiated)
- Remote PE router withdraws the label advertisement
- LSP to the remote PE router goes down
- LDP session with the remote PE router goes down
- Local configuration changes
- Periodic pseudowire OAM procedure fails (Layer 2 circuit-based MPLS ping to the PE router fails)

When you configure a redundant pseudowire between a CE device and a PE router, a periodic (once a minute) ping packet is forwarded through the active pseudowire to verify data plane connectivity. If the ping fails, traffic is automatically switched to the redundant pseudowire.

When a failure is detected, traffic is switched from the failed active pseudowire to the redundant pseudowire. The redundant pseudowire is then designated as the active pseudowire. The switch is nonreversible, meaning that once the redundant pseudowire assumes the role of the active pseudowire at the time of a failover, it remains as the active pseudowire even though the previously active pseudowire comes up again.

For example, a primary pseudowire has failed and traffic has been successfully switched to the redundant pseudowire. After a period of time, the cause of the failure of the primary pseudowire has been resolved and it is now possible to reestablish the original connection. However, traffic is not switched back to the original pseudowire unless a failure is detected on the currently active pseudowire.

Related Documentation

- [Example: Configuring H-VPLS Without VLANs on page 693](#)

Configuring Redundant Pseudowires for Layer 2 Circuits and VPLS

A redundant pseudowire can act as a backup connection between PE routers and CE devices, maintaining Layer 2 circuit and VPLS services after certain types of failures. This feature can help improve the reliability of certain types of networks (metro for example) where a single point of failure could interrupt service for multiple customers. Redundant pseudowires cannot reduce traffic loss to zero. However, they provide a way to gracefully recover from pseudowire failures in such a way that service can be restarted within a known time limit.



NOTE: VPLS is not supported on ACX Series routers.

For an overview of how redundant pseudowires work, see [“Redundant Pseudowires for Layer 2 Circuits and VPLS” on page 177](#).

To configure pseudowire redundancy for Layer 2 circuits and VPLS, complete the procedures in the following sections:

- [Configuring Pseudowire Redundancy on the PE Router on page 180](#)
- [Configuring the Switchover Delay for the Pseudowires on page 180](#)
- [Configuring a Revert Time for the Redundant Pseudowire on page 181](#)

Configuring Pseudowire Redundancy on the PE Router

You configure pseudowire redundancy on the PE router acting as the egress for the primary and standby pseudowires using the **backup-neighbor** statement.

To configure pseudowire redundancy on the PE router, include the **backup-neighbor** statement:

```
backup-neighbor {  
    community name;  
    psn-tunnel-endpoint address;  
    standby;  
    virtual-circuit-id number;  
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary for this statement.

The **backup-neighbor** statement includes the following configuration options:

- **community**—Specifies the community for the backup neighbor.
- **psn-tunnel-endpoint**—Specifies the endpoint address for the packet switched network (PSN) tunnel on the remote PE router. The PSN tunnel endpoint address is the destination address for the LSP on the remote PE router.
- **standby**—Configures the pseudowire to the specified backup neighbor as the standby. When you configure this statement, traffic flows over both the active and standby pseudowires to the CE device. The CE device drops the traffic from the standby pseudowire, unless the active pseudowire fails. If the active pseudowire fails, the CE device automatically switches to the standby pseudowire.
- **virtual-circuit-id**—Uniquely identifies the primary and standby Layer 2 circuits. This option is configurable for Layer 2 circuits only.

Configuring the Switchover Delay for the Pseudowires

To configure the time the router waits before switching traffic from the failed primary pseudowire to a backup pseudowire, include the **switchover-delay** statement:

```
switchover-delay milliseconds;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary for this statement.

Configuring a Revert Time for the Redundant Pseudowire

You can specify a revert time for redundant Layer 2 circuit and VPLS pseudowires. When you have configured redundant pseudowires for Layer 2 circuits or VPLS, traffic is switched to the backup pseudowire in the event that the primary pseudowire fails. If you configure a revert time, when the configured time expires traffic is reverted back to the primary pseudowire, assuming the primary pseudowire has been restored.

To configure a revert time for redundant pseudowires, specify the time in seconds using the **revert-time** statement:

revert-time (Protocols Layer 2 Circuits) *seconds* maximum *seconds*;

With the **maximum** option, specify a maximum reversion interval to add after the **revert-time** delay. If a revert-time delay is defined but a maximum timer is not defined, VCs are restored upon the revert-timer's expiration.

To reduce as much as possible the amount of traffic discarded, and potential data-path asymmetries observed during primary-to-backup transition periods, you can use this restoration timer. This restoration timer is activated when the backup path is performing as active, and then the primary path is restored. The goal is to avoid moving traffic back to the primary path right away, to make sure that the control plane's related tasks (such as IGP, LDP, RSVP, and internal BGP) have enough time to complete their updating cycle.

By enabling a gradual return of traffic to the primary path, you can ensure that the relatively-slow control-plane processing and updating does not have a negative impact on the restoration process.

The **maximum** option extends the revert timer's functionality to provide a jittered interval over which a certain number of circuits can be transitioned back to the primary path. By making use of this maximum value, you can define a time interval during which circuits are expected to switch over. As a consequence, circuits' effective transitions are scattered during restoration periods.

When making use of **revert-time x maximum y** statement, you can ensure that the corresponding circuit that is active is moved to the primary path within a time-slot (t1) such as that: $x \leq t1 \leq y$. In other words, by activating this statement, you can ensure the following:

- VCs stay in the backup path for at least x seconds after the primary path comes back up.
- VCs are moved back to the primary path before y seconds have elapsed.
- y maximum value = x maximum value * 2 = 1200 seconds.

The ideal values for x and y will be conditioned to internal aspects of your network. For this reason, there are no default values for these settings. If no revert-time is set, the default behavior is non-revertive. That is, circuits are not returned to the primary path upon restoration. They are kept on the backup path.

For a list of hierarchy levels at which you can include this statement, see the statement summary for this statement.

**Related
Documentation**

- [Example: Configuring Pseudowire Redundancy in a Mobile Backhaul Scenario on page 371](#)
- [Example: Configuring H-VPLS Without VLANs on page 693](#)

Configuring Class of Service for Layer 2 VPNs

- [Configuring Traffic Policing in Layer 2 VPNs on page 183](#)

Configuring Traffic Policing in Layer 2 VPNs

You can use policing to control the amount of traffic flowing over the interfaces servicing a Layer 2 VPN. If policing is disabled on an interface, all the available bandwidth on a Layer 2 VPN tunnel can be used by a single CCC or TCC interface.

For information on how to configure traffic policers, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*.

To enable Layer 2 VPN policing on an interface, include the **policer** statement:

```
policer {  
    input policer-template-name;  
    output policer-template-name;  
}
```

If you configure CCC encapsulation, you can include the **policer** statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family ccc]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family ccc]

If you configure TCC encapsulation, you can include the **policer** statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family tcc]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family tcc]

For information about how to configure the encapsulation type, see [“Configuring the Encapsulation Type” on page 129](#).

CHAPTER 15

Monitoring Layer 2 VPNs Using BFD

- [Configuring BFD for Layer 2 VPN and VPLS on page 186](#)
- [BFD Support for VCCV for Layer 2 VPNs, Layer 2 Circuits, and VPLS on page 188](#)
- [Configuring BFD for VCCV for Layer 2 VPNs, Layer 2 Circuits, and VPLS on page 188](#)

Configuring BFD for Layer 2 VPN and VPLS

The following procedure describes how to configure Bidirectional Forwarding Detection (BFD) for Layer 2 VPN and VPLS. For VPNs, you configure the BFD sessions on the interfaces carrying traffic from the PE routers to the CE routers.

The BFD protocol is a simple hello mechanism that detects failures in a network. Hello packets are sent at a specified, regular interval. A neighbor failure is detected when the routing device stops receiving a reply after a specified interval. BFD works with a wide variety of network environments and topologies. The failure detection timers for BFD have shorter time limits than default failure detection mechanisms for BGP, so they provide faster detection.

The BFD failure detection timers are adaptive and can be adjusted to be faster or slower. The lower the BFD failure detection timer value, the faster the failure detection and vice versa. For example, the timers can adapt to a higher value if the adjacency fails (that is, the timer detects failures more slowly). Or a neighbor can negotiate a higher value for a timer than the configured value. The timers adapt to a higher value when a BFD session flap occurs more than three times in a span of 15 seconds. A back-off algorithm increases the receive interval by two if the local BFD instance is the reason for the session flap. The transmission interval is increased by two if the remote BFD instance is the reason for the session flap. You can use the **clear bfd adaptation** command to return BFD interval timers to their configured values. The **clear bfd adaptation** command is hitless, meaning that the command does not affect traffic flow on the routing device.

1. You can enable BFD failure detection. The BFD failure detection timers are adaptive and can be adjusted to be faster or slower. The lower the BFD failure detection timer value, the faster the failure detection and vice versa. For example, the timers can adapt to a higher value if the adjacency fails (that is, the timer detects failures more slowly). Or a neighbor can negotiate a higher value for a timer than the configured value. The timers adapt to a higher value when a BFD session flap occurs more than three times in a span of 15 seconds. A back-off algorithm increases the receive (Rx) interval by two if the local BFD instance is the reason for the session flap. The transmission (Tx) interval is increased by two if the remote BFD instance is the reason for the session flap.

To enable BFD failure detection and specify the threshold for the adaptation of the BFD session detection time, specify a time in milliseconds using the **threshold** statement. When the detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.



NOTE: The threshold time must be equal to or greater than the value specified in the **minimum-interval** or the **minimum-receive-interval** statement.

You can use the **clear bfd adaptation** command to return BFD interval timers to their configured values. The **clear bfd adaptation** command is hitless, meaning that the command does not affect traffic flow on the routing device.

2. You can specify the minimum interval after which the local routing device transmits hello packets and then expects to receive a reply from a neighbor with which it has established a BFD session. You specify the interval in milliseconds using the **minimum-interval** statement.

Optionally, instead of using this statement, you can specify the minimum transmit and receive intervals separately using the **minimum-interval** (specified under the **transmit-interval** statement) and **minimum-receive-interval** statements.

3. You can configure the minimum interval after which the local routing device must receive a reply from a neighbor with which it has established a BFD session. Specify the number of milliseconds using the **minimum-receive-interval** statement.
4. You can specify that an interface be declared down when a certain number of hello packets have not been received from a neighboring router through that interface. Specify the number of hello packets by including the **multiplier** statement.
5. You can configure BFD sessions not to adapt to changing network conditions by including the **no-adaptation** statement. We recommend that you *do not* disable BFD adaptation unless it is preferable to have BFD adaptation disabled in your network.
6. Specify the transmit interval options for **bfd-liveness-detection** statement by including the **transmit-interval** statement. The negotiated transmit interval for a peer is the interval between the sending of BFD packets to peers. The receive interval for a peer is the minimum time that it requires between packets sent from its peer; the receive interval is not negotiated between peers. To determine the transmit interval, each peer compares its configured minimum transmit interval with its peer's minimum receive interval. The larger of the two numbers is accepted as the transmit interval for that peer.

The **transmit-interval** statement specifies how often BFD statements are transmitted and includes the following options:

- **minimum-interval milliseconds**—Specify the minimum interval in milliseconds at which the local routing device transmits hello packets to a neighbor with which it has established a BFD session.
- **threshold milliseconds**—Specify the threshold for the adaptation of the BFD session transmit interval. When the transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent.



NOTE: The threshold value specified in the **threshold** statement must be greater than the value specified in the **minimum-interval** statement for the **transmit-interval** statement.

7. Specify the BFD version by including the **version** statement. You can set BFD to version 0, 1, or allow BFD to determine what version it needs to be by including the **automatic** option.

- Related Documentation**
- [bfd-liveness-detection on page 1077](#)
 - [clear bfd adaptation](#)

BFD Support for VCCV for Layer 2 VPNs, Layer 2 Circuits, and VPLS

Bidirectional Forwarding Detection (BFD) support for virtual circuit connectivity verification (VCCV) on MX Series devices enables you to configure a control channel for a pseudowire, in addition to the corresponding operations, administration, and management functions to be used over that control channel.

BFD provides a low resource mechanism for the continuous monitoring of the pseudowire data path and for detecting data plane failures. This feature provides support for asynchronous mode BFD for VCCV as described in RFC 5885, *Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)*. Alternatively, you can use a ping operation to detect pseudowire failures. However, the processing resources required for a ping operation are greater than what is needed for BFD. In addition, BFD is capable of detecting data plane failure faster than a VCCV ping. BFD for pseudowires is supported for Layer 2 circuits (LDP-based), Layer 2 VPNs (BGP-based), and VPLS (LDP-based or BGP-based).

Starting with Release 12.1, Junos OS introduces a distributed model for the BFD for VCCV. Unlike in previous releases where the BFD for VCCV followed a Routing Engine-based implementation, in Release 12.1 and later, the BFD for VCCV follows a distributed implementation over PIC concentrators, such as DPC, FPC, and MPC.

For distributed BFD, you need to configure the lo0 interface with unit 0 and the appropriate family enabled.



NOTE: For the distributed BFD for VCCV to work, you must configure MPLS family (`family mpls`) on the loopback interface.

```
user@router# set interfaces lo0 unit 0 family mpls
```

In Junos OS Release 12.1 and later, the periodic packet management process (ppmd) on the PIC concentrators handles the periodic packet management (send and receive) for BFD for VCCV. This enables Junos OS to create more BFD for VCCV sessions, and to reduce the time taken for error detection. Similarly, the distributed implementation improves the performance of Routing Engines because the Routing Engine resources used for BFD for VCCV implementation become available for Routing Engine-related applications when the BFD for VCCV-related processing moves to the PIC concentrators. The distributed BFD for VCCV implementation also enables the BFD for VCCV sessions to remain across graceful restarts.

Related Documentation

- [Configuring BFD for VCCV for Layer 2 VPNs, Layer 2 Circuits, and VPLS on page 188](#)

Configuring BFD for VCCV for Layer 2 VPNs, Layer 2 Circuits, and VPLS

Bidirectional Forwarding Detection (BFD) support for virtual circuit connection verification (VCCV) allows you to configure a control channel for a pseudowire, in addition to the corresponding operations and management functions to be used over that control

channel. BFD provides a low resource mechanism for the continuous monitoring of the pseudowire data path and for detecting data plane failures.

This feature provides support for asynchronous mode BFD for VCCV as described in RFC 5885, *Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)*. You can also use a ping operation to detect pseudowire failures. However, the processing resources required for a ping operation are greater than what is needed for BFD. In addition, BFD is capable of detecting data plane failure faster than VCCV ping. BFD for pseudowires is supported for Layer 2 circuits (LDP-based), Layer 2 VPNs (BGP-based), and VPLS (LDP-based or BGP-based).

To configure OAM and BFD for Layer 2 VPNs, include the **oam** statement and sub-statements at the **[edit routing-instances *routing-instance-name* protocols l2vpn]** hierarchy level:

```
oam {
  ping-interval ;
  bfd-liveness-detection {
    detection-time {
      threshold milliseconds;
    }
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    multiplier number;
    no-adaptation;
    transmit-interval {
      minimum-interval milliseconds;
      threshold milliseconds;
    }
    version bfd-protocol-version;
  }
  control-channel {
    pwe3-control-word;
    pseudowire-label-ttl-1;
    router-alert-label;
  }
}
```

For more information about how to configure BFD, see the *Junos OS Routing Protocols Library*.

You can configure many of the same OAM statements for VPLS and Layer 2 circuits:

- To enable OAM for VPLS, configure the **oam** statement and substatements at the **[edit routing-instances *routing-instance-name* protocols vpls]** hierarchy level and at the **[edit routing-instances *routing-instance-name* protocols vpls neighbor *address*]** hierarchy level. The **pwe3-control-word** statement configured at the **[edit routing-instances *routing-instance-name* protocols l2vpn oam control-channel]** hierarchy level is not applicable to VPLS configurations.
- To enable OAM for Layer 2 circuits, configure the **oam** statement and substatements at the **[edit protocols l2circuit neighbor *address* interface *interface-name*]** hierarchy level. The **control-channel** statement and sub-statements configured at the **[edit**

routing-instances routing-instance-name protocols [l2vpn oam] hierarchy level do not apply to Layer 2 circuit configurations.

You can use the **show ldp database extensive** command to display information about the VCCV control channel and the **show bfd session extensive** command to display information about BFD for Layer 2 VPNs, Layer 2 circuits, and VPLS.

PART 3

Configuring Group VPNs

- [Configuring Group VPNs on page 193](#)

Configuring Group VPNs

- [Group VPNv2 Overview on page 193](#)
- [Configuring Group VPNs in Group VPNv2 on Routing Devices on page 213](#)
- [Example: Configuring Group VPNs in Group VPNv2 on Routing Devices on page 216](#)

Group VPNv2 Overview

- [Group VPNv2 Technology Overview on page 193](#)
- [Group VPNv2 Implementation Overview on page 201](#)

Group VPNv2 Technology Overview



NOTE: Group VPNv2 is the name of the Group VPN technology on MX5, MX10, MX40, MX80, MX240, MX480, and MX960 routers. Group VPNv2 is different from the Group VPN technology implemented on SRX Security Gateways. The term Group VPN is sometimes used in this document to refer to the technology in general, not to the SRX technology.

For more information about Group VPN on SRX Security Gateway devices, see *Group VPNv2 Overview*.

This section explains the technological concepts of Group VPNv2.

- [Understanding Group VPNv2 on page 194](#)
- [Group VPNv2 and Standard IPsec VPN on page 194](#)
- [Understanding the GDOI Protocol on page 196](#)
- [GDOI Protocol and Group VPNv2 on page 198](#)
- [Group VPNv2 Traffic on page 199](#)
- [Group Security Association on page 199](#)
- [Group Controller/Key Server on page 199](#)
- [Group Member on page 200](#)
- [Anti-Replay Protection for Group VPNv2 Traffic on page 200](#)
- [Partial Fail-Open on MX Series Member Routers on page 200](#)

Understanding Group VPNv2

Group VPNv2 is a category of VPN that eliminates the need for point-to-point VPN tunnels in a mesh architecture. It is a set of features that are necessary to secure IP multicast group traffic or unicast traffic over a private WAN that originates on or flows through a router.

Group VPNv2 introduces the concept of a trusted group to eliminate point-to-point tunnels and their associated overlay routing. All group members share a common security association (SA), also known as a group SA. This enables group members to decrypt traffic that was encrypted by any other group member.

Group VPNv2 provides the following advantages:

- Provides data security and transport authentication, helping to meet security compliance and internal regulation by encrypting all WAN traffic.
- Enables high-scale network meshes and eliminates complex peer-to-peer key management with group encryption keys.
- Reduces the number of endpoint changes that need to be made due to group member change or policy change.
- Maintains network intelligence such as full-mesh connectivity, natural routing path, and quality of service (QoS) in MPLS networks.
- Grants authenticated membership control with a centralized key server.
- Allows encryption and decryption of traffic among all group members defined in the group policy.
- Helps to ensure low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub.
- Reduces traffic loads on customer premises equipment (CPE) and provider edge (PE) encryption devices by using the core network for replication of multicast traffic, avoiding packet replication at each individual peer site.

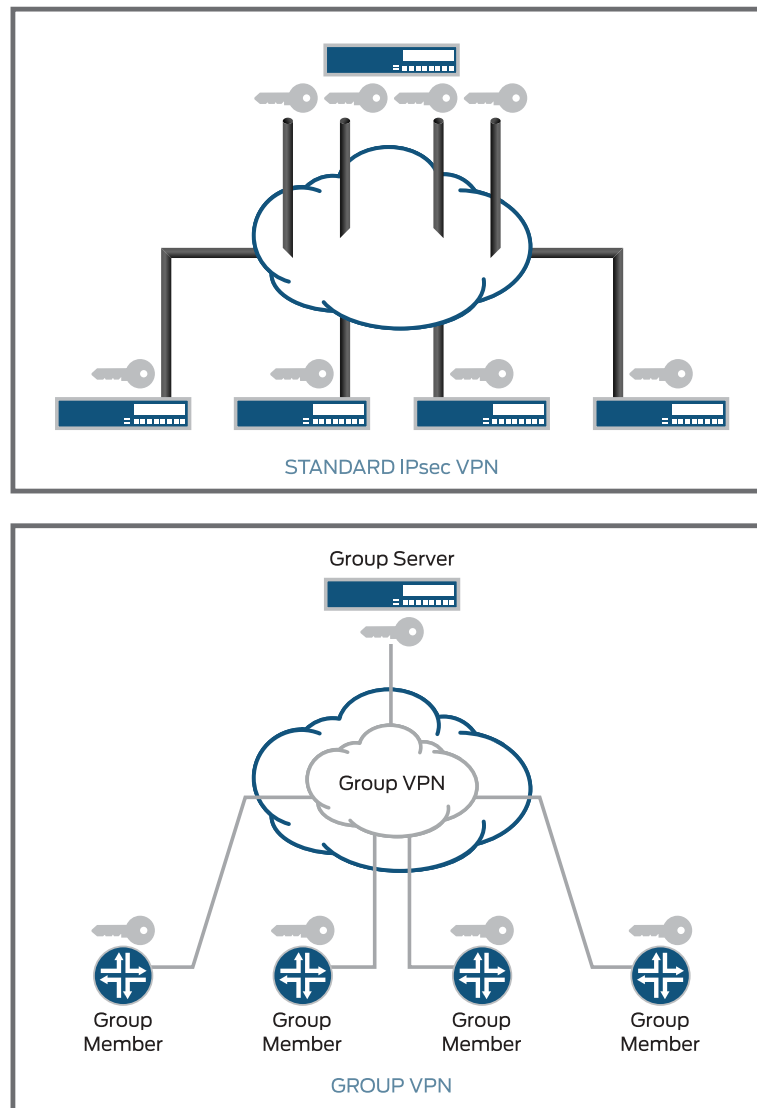
Group VPNv2 and Standard IPsec VPN

Group VPNv2 is built on standards-based technologies that integrate routing and encryption together in the network. An IPsec security SA is a unidirectional agreement between VPN participants that defines the rules to use for authentication and encryption algorithms, key exchange mechanisms, and secure communications.

Traditional IPsec VPN deployments tackle the problem of securing traffic between gateways in the network by creating an overlay network based on the use of point-to-point tunnels. Traffic carried over these tunnels is normally encrypted and authenticated in order to provide data integrity and confidentiality. Secure group members are managed through the Group Domain of Interpretation protocol (GDOI). The GDOI solution takes a different approach by disassociating the encryption and authentication problem from the transport. By doing this, GDOI-based solutions provide a way to encrypt branch-to-branch communications without the need to configure branch-to-branch tunnels.

With current VPN implementations, the SA is a point-to-point tunnel between two end points. Group VPNv2 extends the IPsec architecture to support SAs that are shared by a group of routers (see [Figure 13 on page 195](#)). A key server distributes keys and policies to all registered and authenticated member routers. By distributing policies from a centralized point and by sharing the same group security association (the entire group has a single Phase 2 SA) with authenticated group members, key distribution and management are greatly simplified.

Figure 13: Standard IPsec VPN and Group VPNv2



Group VPNv2 is a client/server architecture. All members have a unique Phase 1 IKE SA with the key server. Hence, if there are n members, there is a total of n Phase 1 IKE SAs. However, the entire group shares a single Phase 2 SA.

In traditional IPsec, the tunnel endpoint addresses are used as a new packet source and destination. The packet is then routed over the IP infrastructure, using the encrypting end

point source IP address and the decrypting end point destination IP address. In the case of Group VPN, IPsec-protected data packets preserve the original source and destination addresses of the host in the outer IP header in order to preserve the IP address. This is known as tunnel header preservation. The biggest advantages of tunnel header preservation is the ability to route encrypted packets using the underlying network routing infrastructure.

Thus, with Group VPNs, any-to-any connectivity is achieved by preserving the original source and destination IP addresses in the outer header. Secure multicast packets are replicated in the same way as cleartext multicast packets in the core network. The external IP header in the Group VPN is an exact copy of the IP header of the original packet within the ESP header, whereas the external IP header in a traditional VPN contains the IP addresses of the VPN gateways.

Table 7: Group VPN vs Traditional Point-to-Point IPsec

Feature	Traditional Point-to-Point IPsec Tunnels	Group VPN
Scalability	IKE/IPsec tunnels between each pair of peers increases management and configuration complexity.	Single SA and key pair used for the entire any-to-any group. Reduced management and configuration complexity.
Any-to-any instant connectivity	Cannot be done to scale due to management and configuration complexity.	Scales well due to the use of GDOI and shared SA within the group.
Overlay routing	Requires overlay routing.	No overlays-native routing.
IP Header Preservation	New IP Header added to original packet results in limited advanced quality of service (QoS). Will work in NAT environments.	Keeps original IP header on IPsec packet. Preserves advanced QoS capabilities. Will not work in NAT environments.

Understanding the GDOI Protocol

The Group Domain of Interpretation (GDOI) protocol described in RFC 6407 is used to distribute a set of cryptographic keys and policies to a group of devices. GDOI is defined as the Internet Security Association Key Management Protocol (ISAKMP) Domain of Interpretation (DOI) for group key management. In a group management model, the GDOI protocol operates between a group member and a group controller or key server (GC/KS) and manages group security associations and group-keys for a set of security participants. The ISAKMP defines two phases of negotiation. GDOI is a Phase 2 protocol protected by a Phase 1 ISAKMP security association. IKEv1 is specified in RFC 6407 as a Phase 1 protocol.

GDOI introduces two different encryption keys:

- Key encryption key (KEK)—Used to secure the control plane. KEK is the name of the key used by the group members to decrypt rekey messages from the GC/KS. This key is part of the Security Association Key Encryption Key (SAK).
- Traffic encryption key (TEK)—Used to secure the data plane. TEK is the name of the key used by the group members to encrypt or decrypt communication between other

group members. This key is part of the Security Association Transport Encryption Key (SA TEK).

As with standard IPsec, all keys have a lifetime and have to be rekeyed. The keys distributed through GDOI are group keys and are used by the entire group.

The group SAs and key management are handled through two types of GDOI exchanges:

- **groupkey-pull**—This exchange allows a member to request SAs and keys shared by the group from the server.

In the pull method, the group member requests the group SA and policy from the key server. This request is protected over the IKE SA.

The **groupkey-pull** is the first exchange in the GDOI protocol and is used for group member registration with the GC/KS. The group member specifies the group with which it wants to register, and the GC/KS sends all necessary group SAs and keys to the group member if the member is authorized to join the group. The complete exchange is secured by a Phase 1 SA (IKEv1 SA), which is established with IKEv1 before the **groupkey-pull** exchange begins. The **groupkey-pull** is part of Phase 2 of the GDOI protocol.

- **groupkey-push**—This exchange is a single rekey message that allows the server to send group SAs and keys to members before existing group SAs expire. Rekey messages are unsolicited messages sent from the server to members.

The **groupkey-push** is the second exchange in the GDOI protocol and is initiated by the GC/KS to all registered members of the group. [Table 8 on page 197](#) shows the payloads that the MX Series group member expects to receive in **groupkey-push** messages.

Table 8: groupkey-push Message Payloads

Payload	Description
group associated policy (GAP)	A GAP payload allows for the distribution of group-wide policy, such as instructions as to when to activate and deactivate SAs. This payload contains values for activation time delay (ATD) and deactivation time delay (DTD) for the traffic encryption key (TEK) as well as IP-Delivery Delayed Detection Protocol window type and window size for the IPsec traffic.
Security Association Transport Encryption Key (SA TEK)	Traffic selectors.
Security Association Key Encryption Key (SAK) (Optional)	The security association (SA) for the key encryption key (KEK). Also known as SA KEK. NOTE: groupkey-push messages that do not include the optional payloads are still valid messages.
traffic encryption key (TEK) (Optional)	Key for encrypting the data traffic between group members.
key encryption key (KEK) (Optional)	Used to protect the TEK.

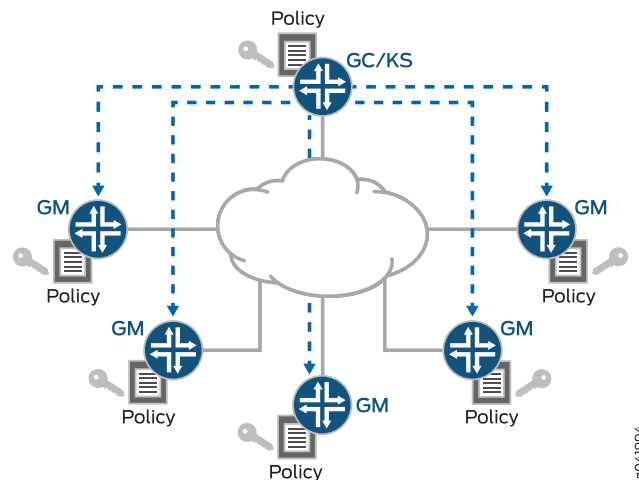
The **groupkey-push** exchange is secured by an SA KEK (SAK), which is installed during the **groupkey-pull** exchange. The **groupkey-push** is part of Phase 2 of the GDOI protocol.

GDOI Protocol and Group VPNv2

Group VPNv2 is the name of the security technology implemented on the MX5, MX10, MX40, MX240, MX480, MX960 routers from Juniper Networks. Group VPNv2 uses the GDOI protocol (RFC 6407) as a base, in addition to other functionalities.

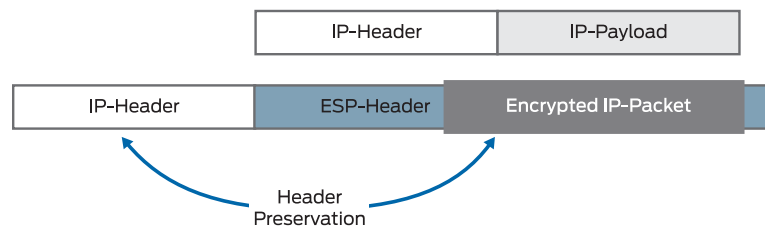
Group VPNv2 technology is based on the GDOI protocol to handle the most important functionality. This protocol is specified in RFC 6407 and defines an ISAKMP Domain of Interpretation (DOI) to manage group SAs and keys for a group of security participants. Thus, all members of the group share identical information to encrypt and decrypt traffic among each other. The creation, management, and distribution of group SAs and group keys are centralized and performed by the GC/KS. [Figure 14 on page 198](#) provides a brief overview of the Group VPNv2 functionality using GDOI.

Figure 14: Group VPNv2 Using GDOI



The group members use the Encapsulating Security Payload (ESP) protocol in tunnel mode to secure the traffic. However, in Group VPN the tunnel mode is modified. Because there is no direct association between the group members, it is not necessary to use special IP addresses in the outer IP header (that is, IP addresses of IPsec gateways). Every group member can decrypt the traffic of every other group member. Thus, the inner IP-Header is copied to the outer IP-Header, and the underlying routing infrastructure and QoS infrastructure can be used. This feature is called Header Preservation and is shown in [Figure 15 on page 199](#).

Figure 15: Header Preservation



To get group SAs and group keys, the group member must register with the GC/KS for a specific group. The result is an IKEv1 SA, which is only needed to secure the registration process. After the registration, the group member has all the information to communicate with the other group members (SA TEK), as well as the information to successfully decrypt the rekeying messages (SAK). The GC/KS sends out rekeying messages before either the SA TEK or SAK lifetime expires. It is also possible to send an SA TEK update as well as a SAK update in the same rekey message. The IKEv1 SA is no longer needed and is deleted after the lifetime expires (no IKEv1-rekeying).

Group VPNv2 Traffic

Group VPNv2 traffic includes:

- Control-plane-traffic—Traffic from the group members to the GC/KS in the Group VPNv2 deployment with the GDOI protocol only.
- Data-plane-traffic—Traffic between the group members in the Group VPNv2 deployment with the ESP protocol only which is already known from IPsec.

Group Security Association

Unlike traditional IPsec encryption solutions, Group VPN uses the concept of group security association. A group SA is similar to an SA in terms of functionality. Group SAs are shared among all group members of a common GDOI group. All members in the Group VPN group can communicate with each other using a common encryption policy and a shared group SA. With a common encryption policy and a shared group SA, there is no need to negotiate IPsec between group members. This reduces the resource load on the group members. Traditional IPsec scalability issues (number of tunnels and associated SAs) do not apply to Group VPN group members.

Group Controller/Key Server

A group controller or key server (GC/KS) is a device used for creating and maintaining the Group VPNv2 control plane. It is responsible for creation and distribution of group SAs and group keys. All information the group members need to communicate with other group members is provided by the GC/KS. All encryption policies, such as interesting traffic, encryption protocols, security association, rekey timers, and so on, are centrally defined on the GC/KS and are pushed down to all group members at registration time. Group members authenticate with the GC/KS using IKE Phase 1 and then download the encryption policies and keys required for Group VPN operation. The GC/KS is also responsible for refreshing and distributing the keys.



NOTE: The GC/KS functionality is not supported on MX Series routers. The MX Series routers that are configured as group members can connect with Cisco GC/KS only. There is no support for MX Series group members to interact with the Juniper Networks SRX Series acting as GC/KS. See [Table 11 on page 212](#) for compatibility between the various types of group members and GC/KSs.

Group Member

A group member is an IPsec endpoint device used for the traffic encryption process and is responsible for the actual encryption and decryption of data traffic. A group member is configured with IKE Phase 1 parameters and GC/KS information. Encryption policies are defined centrally on the GC/KS and downloaded to the group member at the time of successful registration. Each group member then determines whether incoming and outgoing traffic should be decrypted or encrypted (using its SA) based on its group membership.

From a functionality point of view, a group member is similar to an IPsec gateway. However, the SAs in normal IPsec exist between two IPsec gateways. In GDOI, the group member registers with the GC/KS in order to participate in the Group VPN. During registration, the group member provides the group ID to the GC/KS to get the respective policies, SAs, and keys needed for this group. Rekeying is accomplished by the group members through the **groupkey-pull** method (re-registration) or by the GC/KS through the **groupkey-push** method.

Anti-Replay Protection for Group VPNv2 Traffic

Since Group VPN communication is essentially any-to-any communication over the same shared security association, the use of sequence numbers for anti-replay protection does not work. Because of this, Junos OS supports an IETF draft specification for a time-based anti-replay mechanism, draft-weis-delay-detection-01. It is available at <http://tools.ietf.org/html/draft-weis-delay-detection-01>.

To implement this feature, MX Series member routers make use of a new IP Delivery Delay Detection Protocol time-stamp header within the packet. See [“Implementing IP Delivery Delay Detection Protocol \(Time-Based Anti-Replay Protection\)” on page 207](#) for details.

Partial Fail-Open on MX Series Member Routers

Group members in a Group VPN rely on the GC/KS to generate keying material for the shared SA. Therefore, connectivity between the group members and GC/KSs is required to initially protect traffic and to continually protect traffic over rekey events. In the event of communication failure between the group member and the GC/KS, the default behavior of the group members is to stop forwarding traffic. This is known as fail-closed.

A nondefault configuration option is available to permit some specifically defined traffic to flow through the group member without being encrypted until such time as the member is able to contact the GC/KS and retrieve the active SA. This is known as partial fail-open.

The partial fail-open feature requires a policy configuration option that creates a rule on the applicable MX Series group member for a particular Group VPNv2 defined by source and destination addresses. This fail-open rule is active only when group SA is in disabled state because of connectivity failure with the key server. Traffic that would normally pass through the Group VPN but does not match the fail-open rule is dropped. More than one fail-open rule can be defined for the Group VPN object. If no fail-open rules are configured, then the fail-open feature is disabled.

Group VPNv2 Implementation Overview

This section explains the Juniper Networks solution for implementing Group VPNv2.

- [Enabling Group VPNv2 on page 201](#)
- [Registering a Group Member on page 202](#)
- [Rekeying a Group Member \(groupkey-push Method\) on page 203](#)
- [Rekeying a Group Member \(groupkey-pull Method\) on page 204](#)
- [Authenticating a Group Member on page 205](#)
- [Fragmenting Group VPNv2 Traffic on page 205](#)
- [Encrypting Group VPNv2 Traffic on page 206](#)
- [Decrypting Group VPNv2 Traffic on page 206](#)
- [Configuring a Routing Instance for Group VPNv2 on page 207](#)
- [Establishing Multiple Groups, Policies, and SAs on page 207](#)
- [Connecting with Multiple Cooperative GC/KSs on page 207](#)
- [Implementing IP Delivery Delay Detection Protocol \(Time-Based Anti-Replay Protection\) on page 207](#)
- [Changing Group VPNv2 Configuration on page 208](#)
- [Bypassing Group VPNv2 Configuration on page 208](#)
- [Implementing Partial Fail-open on MX Series Member Routers on page 208](#)
- [Supported GDOI IPsec Parameters on page 209](#)
- [Supported GDOI IKEv1 Parameters on page 210](#)
- [Applying Dynamic Policies on page 211](#)
- [Supporting TOS and DSCP on page 211](#)
- [Interoperability of Group Members on page 211](#)
- [Group VPNv2 Limitations on page 212](#)

Enabling Group VPNv2

A service set is used to enable Group VPNv2 on a particular interface on applicable MX Series routers.

- [Configuring the Service Set on page 202](#)
- [Applying the Service Set on page 202](#)
- [Packet Steering on page 202](#)

Configuring the Service Set

Group VPNv2 is configured inside a service set using the **ipsec-group-vpn** statement at the **[edit services service-set service-set-name]** hierarchy level.

Sample Service Set Configuration

```
[edit services]
service-set service-set-name {
  interface-service {
    service-interface service-interface-name;
  }
}
ipsec-group-vpn vpn-name;
```



NOTE:

- Only one group member can be configured per service set.
- Next-hop style service set is not supported with Group VPNv2.

Applying the Service Set

A service set is applied at the interface level.

Sample Applying Service Set Configuration

```
[edit interfaces]
interface-name {
  unit 0 {
    family inet {
      service {
        input {
          service-set service-set-name;
        }
        output {
          service-set service-set-name;
        }
      }
      address 10.0.30.2/30;
    }
  }
}
```

Packet Steering

The interface-style service set configuration is used to steer traffic from the Packet Forwarding Engine to the PIC. Packets received on an interface with a service set pointing to the Group VPNv2 object are forwarded to the PIC by being injected into the corresponding service interface.

Registering a Group Member

The group member registration to the server starts when the **ipsec-group-vpn** statement is configured for a service set and the service interface is up. When the service interface

goes down, all group SAs associated with this interface are cleared, and no registration is triggered for these Group VPNs until the interface comes up.

Group member registration involves establishing IKE SA with the GC/KS followed by a **groupkey-pull** exchange to download the SAs and the traffic keys for the specified group identifier.



NOTE: Junos OS does not support traffic-based SA negotiation triggering for Group VPNs in Group VPNv2.

Rekeying a Group Member (groupkey-push Method)

The GC/KS will send out a unicast **groupkey-push** message to registered group members in order to:

- Send new key encryption keys (KEKs) or traffic encryption keys (TEKs).

The push messages can contain all or only some of the payload elements shown in [Table 8 on page 197](#). When the GAP payload contains both old SAs and new replacement SAs, the group member router will apply the ATD and DTD values as a normal rekey by means of push. If there is no ATD value in the update, the member router installs the new SAs immediately. If there is no DTD value, the old SAs will remain in place until their expiration.

- Update group associated policy (GAP) for an existing SA.

A GC/KS can send a unicast push message to update the configuration to group members at any time. The GAP payload can include configuration changes to the IP Delivery Delay Detection Protocol, encryption algorithm, lifetime, and so on. The updated configuration is either applied immediately or with a delay. ATD and DTD values are used to achieve the timing for the activation of the new TEK and deletion of the existing TEK, respectively. If the existing TEK lifetime has to be reduced, then the DTD value is set accordingly in the push message. The new TEK in the push message is activated based on the ATD value in the payload.

- Send delete key notifications for TEK or KEK.

The GC/KS can send the optional delete notification payload in the push message for deleting keys and SAs on the member. The push message contains the protocol ID that indicates whether the delete notification is for TEK or KEK. The group member router deletes the key based on the group ID and SPI value contained in the payload. Deleting a specific TEK or KEK can be done with a delay value specified in the DTD attribute. If the delay value is 0, and the payload contains a specific SPI, then the matching TEK or KEK is deleted immediately. If all the TEKs or KEKs (or both) need to be deleted in the group, then the SPI value is set to 0 for the corresponding protocol ID in the payload.

- Remove a member router from the Group VPN in Group VPNv2.

The push messages are used to allow the GC/KS to delete members from the Group VPN. In one case, the GC/KS sends a rekey message with only the old SAs and a smaller DTD value. The group member router installs the new, smaller DTD value. Since it did

not receive new SA keys, the member router tries to re-register using the **groupkey-pull** method. This re-registration attempt is rejected by the GC/KS, thus deleting the member from the Group VPN. In the second case, the GC/KS sends a delete payload for the SPI of the old SA. The group member router deletes the SA immediately and attempts to re-register using the **groupkey-pull** method. This re-registration attempt is rejected by the GC/KS, thus deleting the member from the Group VPN.

Registered MX Series group members send a unicast PUSH ACK message back to the GC/KS to acknowledge the receipt of the original push message.

Rekeying a Group Member (groupkey-pull Method)

For group member rekeying, using the **groupkey-pull** method, the group members typically re-register with the GC/KS when there is between 7 percent and 5 percent remaining in the existing TEK or KEK soft lifetime. If the existing IKE SA is available, it is used in the pull message. After the GC/KS responds with a new key, both the old key and the new key can be used for decryption. However, the new key is not used for encryption until 30 seconds of lifetime of the old key is remaining. If the existing IKE SA is not available, the pull message results in new IKE negotiations between the group member and the GC/KS.

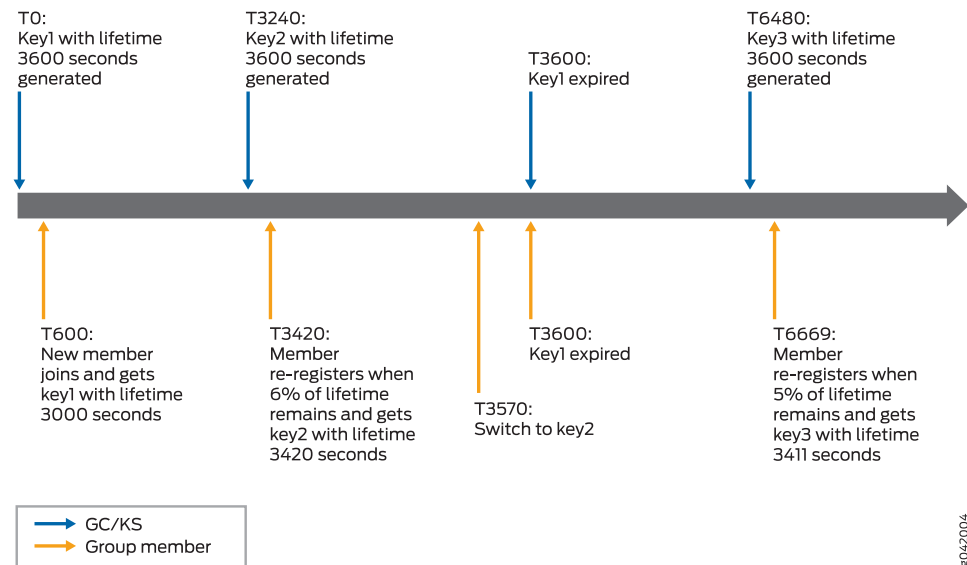
Upon receiving the pull message regarding a specific Group VPN from the group member, the GC/KS responds with all the TEKs and the KEK for that group.

If any existing SA is not included in the response from the GC/KS, then the missing SAs are deleted by the group member.

Taking as an example, the GC/KS is configured with a lifetime of 3600 seconds and is connected to one group member without retransmit. Based on the server configuration, the GC/KS generates a new key when 10 percent of the lifetime is remaining. The group member, however, re-registers with the GC/KS when 5 percent to 7 percent of the lifetime is remaining.

[Figure 16 on page 205](#) represents the rekeying process between the GC/KS and the group member.

Figure 16: Group Member Rekeying



Authenticating a Group Member

Junos OS does not provide public key infrastructure (PKI) support for Group VPN in Group VPNv2. As a result, pre-shared keys are used for group member authentication.

Fragmenting Group VPNv2 Traffic

Because of the header preservation functionality and the usage of the underlying routing infrastructure, it is necessary to fragment the packets before encryption occurs (if it cannot be prevented).

Hence, pre-fragmentation is supported and is recommended for all deployments.

To avoid post-fragmentation, set the **clear**, **set**, and **copy** options for the DF bit in the Group VPNv2 configuration.

Based on this flag setting, the IPsec header has either the **df-bit** set to **clear**, **set**, or **copy** from the inner packet.



NOTE: The DF bit has the clear option set as default.

Sample DF Bit Configuration

```
[edit]
security {
  group-vpn {
    member {
      ipsec {
        vpn group-vpn-name {
          df-bit clear;
        }
      }
    }
  }
}
```

Encrypting Group VPNv2 Traffic

Group members encrypt traffic based on the group SAs and keys provided by the GC/KS. The Group VPNv2 encryption path is as follows:

1. Packet received by the Packet Forwarding Engine is checked against a flow match. If a match is found, the packet is further processed and transmitted.
2. If a match is not found, a rule lookup is performed. If a match is found, a flow is created, and the packet is further processed and transmitted.
3. If the rule lookup fails, the packet is dropped.



NOTE: Group SA is not triggered during packet processing.

Decrypting Group VPNv2 Traffic

After registration is successful and Group VPN SAs are installed, an ESP session is created. Group VPNv2 creates the ESP session with a zero source and destination IP. Because the ESP session is already created at SA installation, packets are expected to match the existing ESP session.

The Group VPNv2 decryption path is as follows:

1. Packet received by the Packet Forwarding Engine undergoes a fragmentation check. If the packet is fragmented, it is assembled for further processing.
2. After packet assembling or if the packet is not fragmented, a zero source and destination IP is used in the 5-tuple decrypt flow lookup. If a match is found, the packet is further processed and transmitted.
3. If the decrypt flow lookup fails, the packet is checked against an SPI flow with zero source and destination IP.

4. If the SPI flow lookup fails, the packet is dropped.
5. If an SPI flow match is found, a decrypt flow is created to avoid the SPI flow lookup for subsequent packets.

Configuring a Routing Instance for Group VPNv2

Routing instances are supported for both control and data traffic. To enable routing instance support on control plane traffic for a group member to reach the GC/KS in a given VRF routing instance, add the **routing-instance** statement at the **[edit security group-vpn member ike gateway gateway-name local-address address]** hierarchy level.

No additional CLI is required to support a routing instance for data-plane packets, as it is determined based on the media interface on which the service set is applied.

Establishing Multiple Groups, Policies, and SAs

Junos OS provides support for one Group VPN per service set in Group VPNv2. However, multiple service sets can be created to support multiple groups in a routing instance. Multiple SAs can be configured per group. However, multiple policies for the same traffic key/SPI is not supported. If the server sends two policies for the same TEK, then they must be paired to be accepted, for instance, A-B and B-A, where A and B are IP addresses or subnets. If multiple unpaired policies for a given TEK are received, registration fails and a system log message is generated.

Connecting with Multiple Cooperative GC/KSs

For a group member to work with a GC/KS in the cooperative mode, the configuration is extended to allow a maximum of four servers in the server list.

During rekeying when using the **groupkey-pull** method, the group member tries to connect to the GC/KS. When the connection to the GC/KS fails, the group member tries to reconnect to the GC/KS. After three retries with an interval of 10 seconds, if the connection to the GC/KS is not restored, the group member tries to establish a connection with the next available server on the server list. This process is repeated until the group member connects to a GC/KS. During this time, the unexpired GDOI SAs on the group members are not cleaned up, so Group VPN traffic is not affected. The time gap between rekeying and hard lifetime expiry provides sufficient time for the group members to connect to the next available server, in such cases.

Implementing IP Delivery Delay Detection Protocol (Time-Based Anti-Replay Protection)

There is no configuration needed to implement the IP Delivery Delay Detection Protocol. MX Series group members get the replay window size to use as a part of the GAP payload in push or pull messages from the key server. If the received window size is 0, time-based anti-replay protection is disabled.

If IP Delivery Delay Detection Protocol is enabled, the sender adds its current timestamp and encrypts the packet. The receiver decrypts the packet and compares its current time with the timestamp in the packet. Packets that fall outside of the window size are dropped.

Because of this, all group members should have their clocks synchronized using Network Time Protocol (NTP).

IP Delivery Delay Detection Protocol times are measured in seconds. See [IP Delivery Delay Detection Protocol-draft-weis-delay-detection-01](#) for more information.



NOTE: All latency issues associated with NTP also apply within IP Delivery Delay Detection Protocol. Thus, a minimum window size of 1 second is recommended.

Changing Group VPNv2 Configuration

Most Group VPNv2 configuration changes result in deleting both existing SAs and re-registration. This triggers both phase 1 and SA download with new traffic keys.

Bypassing Group VPNv2 Configuration

If certain traffic like a routing protocol needs to bypass a Group VPN in Group VPNv2, a service filter needs to be configured on the interface on which the service set is applied. Packets matching the service filter do not come to the PIC for service processing and are directly forwarded to the Routing Engine.

Sample Service Set Filter Configuration

```
[edit interfaces]
interface-name {
  unit 0 {
    family inet {
      service {
        input {
          service-set service-set-name service-filter filter-name;
        }
        output {
          service-set service-set-name service-filter filter-name;
        }
      }
    }
  }
}
```

Implementing Partial Fail-open on MX Series Member Routers

By default, packets are dropped if a group member router is unable to get SAs from the GC/KS due to loss of connectivity. If you want to allow some traffic to pass unencrypted in the event of a communication failure between the group member and the GC/KS, you must configure a **fail-open** rule at the `[edit security group-vpn member ipsec vpn vpn-name]` hierarchy level.

Fail-open rules will be applied to the traffic only in the event of loss of server connectivity. Fail-open rules will be deactivated once connectivity is restored and keys are received from the GC/KS.

Sample Fail-Open Rule Configuration

```
[edit security group-vpn member ipsec vpn vpn-name]
fail-open {
  rule rule-name{
    source-address source-ip-address
    destination-address destination-ip-address}
  }
}
```

A maximum of 10 fail-open rules can be configured for any given group.

Supported GDOI IPsec Parameters

Every GDOI group has a unique ID. It is used as a common base between GC/KS and the group member to communicate about group SAs and group keys.

During the registration process, the GC/KS sends Security Association Transport Encryption Keys (SA TEKs) to the group members. All parameters regarding the whole group security policy are configured on the GC/KS. The SA TEK is used by the group members to protect the traffic exchanged among each other. [Table 9 on page 209](#) shows the parameters of the SA TEK.

Table 9: SA TEK Parameters

Parameters	Supported Values
Encryption	<ul style="list-style-type: none"> • DES-CBC • 3DES-CBC • AES-CBC 128 • AES-CBC 192 • AES-CBC 256
Integrity	<ul style="list-style-type: none"> • HMAC-MD5-96 • HMAC-SHA1-96 • HMAC-SHA-256-128
Lifetime	Any supported value

Besides the cryptographic algorithms, the traffic, which should be encrypted by the group members, is part of the SA TEK policy (traffic selector).

The following statements can be used on a Juniper Networks group member. Thus, the addresses have to be specified under the IKE hierarchy level. The enumeration is also prioritized. Thus, in the following example configuration, KS1 is contacted before KS2.

Sample GDOI IPsec Parameters Configuration

```
[edit security]
group-vpn {
  member {
    ike {
      gateway gateway-name {
        ike-policy policy-name;
        server-address <IP_KS1> <IP_KS2> <IP_KS3> <IP_KS4>;
        local-address <IP_GM> routing-instance routing-instance-name;
      }
    }
  }
  ipsec {
    vpn vpn-group-name {
      ike-gateway gateway-name;
      fail-open {
        rule rule-name {
          source-address 198.51.100.1/24
          destination-address 192.0.2.1/24
        }
      }
      group group-ID;
      match-direction output;
    }
  }
}
```

Supported GDOI IKEv1 Parameters

The group members use only IKEv1 during the registration process in the Group VPNv2 environment. [Table 10 on page 210](#) provides an overview of the defined parameters of the IKEv1 SA.

Table 10: IKEv1 SA Parameters of Group Member

Parameter	Supported Values
Encryption	<ul style="list-style-type: none"> DES-CBC 3DES-CBC AES-CBC 128 AES-CBC 192 AES-CBC 256
Authentication	Pre-shared key (minimum 20 signs)
Integrity	<ul style="list-style-type: none"> MD5 SHA1 SHA256

Table 10: IKEv1 SA Parameters of Group Member (*continued*)

Parameter	Supported Values
Diffie-Hellman Group	<ul style="list-style-type: none"> Group 1 Group 2 Group 5 Group 14
Lifetime	Any supported value

The above-mentioned IKEv1 standards are configured as follows:

Sample IKEv1 Configuration

```
[edit security]
group-vpn {
  member {
    ike {
      proposal proposal-name {
        authentication-algorithm sha1;
        authentication-method pre-shared-keys;
        dh-group group5;
        encryption-algorithm aes-128-cbc;
        lifetime-seconds 3600;
      }
      policy policy-name {
        mode main;
        proposals proposal-name;
        pre-shared-key ascii-text "SECRET DATA";
      }
    }
  }
}
```

Applying Dynamic Policies

The **input** and **output** options under the **ipsec-group-vpn** statement specify if the dynamic policies received from the server are used when the interface on which the service set is applied is the incoming or outgoing interface. This provides flexibility to specify different rules in the incoming and outgoing directions.

Supporting TOS and DSCP

Type of service (TOS) and DiffServ Code Points (DSCP) bits are copied from the inner packet to the ESP packet.

Interoperability of Group Members

Cisco's implementation of GDOI is called Group Encryption Transport (GET) VPN. While Group VPNv2 in Junos OS and Cisco's GET VPN are both based on RFC 6407, *The Group Domain of Interpretation*, there are some implementation differences that you need to be aware of when deploying GDOI in a networking environment that includes both Juniper

Networks security and routing devices and Cisco routers. For more information, see the current Junos OS release notes.

Group VPNv2 interoperability is as follows:

- Junos OS provides interoperability support with Cisco IOS GC/KS support.
- Junos OS does not provide support for Group VPNv2 interoperability with the SRX Series Group VPN server.

Table 11: Group VPNv2 Interoperability

Group Member	SRX Group Member	MX Group VPNv2 Member	Cisco Group Member	SRX GC/KS	Cisco GC/KS
MX Group VPNv2 Member	No	Yes	Yes	No	Yes
SRX Group Member	Yes	No	No	Yes	Yes

Junos OS does not support the deny policy used on a Cisco GC/SK server to add an exception to the group policy. As a workaround, this can be done by configuring firewall rules on an MX Series group member. Also, Junos OS group members can work with the deny policy by not failing the negotiation and simply ignoring the contents. This allows system administrators to easily manage networks where both Cisco group members and Junos OS group members co-exist.

Group VPNv2 Limitations

Junos OS Group VPNv2 does not provide support for the following:

- Multicast push messages
- Multicast traffic
- GDOI SNMP MIBs
- Protocol and port in the policies sent by the server. The group member honors only the IP address/subnet specified in the policy.
- Multiple unpaired policies for the same traffic key/SPI
- Overlapping of both local and remote IP across routing instances in an IKE gateway configuration
- Overlapping Group VPNv2 policies that can result in mismatched SAs
- IPv6 for control and data traffic
- Co-existence of IPsec and Group VPN on the same service set
- Co-existence of services like NAT and ALG on the same service set. NAT and Group VPN can co-exist on different service sets. However, they cannot co-exist on the same service set.
- Site To Site (S2S) VPN and dynamic end point (DEP) VPN can co-exist with Group VPN on different service sets. However, they cannot co-exist on the same service set.

- Multiple groups on same service set
- Group member support with SRX Series GC/KS
- Group member support with SRX Series group member
- Logical Key Hierarchy (LKH)
- Graceful restart
- High availability
- Unified ISSU
- PKI support for authentication
- AMS interface and load-balancing support

**Related
Documentation**

- [Example: Configuring Group VPNs in Group VPNv2 on Routing Devices on page 216](#)

Configuring Group VPNs in Group VPNv2 on Routing Devices

You can configure an MX Series router with MS-MIC-16G and MS-MPC-PIC line cards to provide the Group VPNv2 member functionality support with one or more Cisco group controllers or key servers (GC/KSs). The group members can connect to a maximum of four Cisco GC/KSs with minimum interoperability with the cooperative servers.

The Group VPNv2 feature also provides system logging support for the Group VPNv2 functionality, and routing instance support for both control and data traffic.

Before you begin:

1. Configure the routers for network communication.
2. Configure the Cisco GC/KS.
3. Configure the group member device interfaces.
4. Configure a static route to reach the group server.

To configure a Group VPNv2 member, complete the following tasks:

1. In configuration mode, go to the following hierarchy level:

```
[edit]
user@GM1# edit security
```

2. Define the IKE proposal.

```
[edit security]
user@GM1# set group-vpn member ike proposal proposal-name
```

3. Configure the Phase 1 SA for the IKE proposal.

```
[edit security]
user@GM1# set group-vpn member ike proposal proposal-name authentication-method
pre-shared-keys
user@GM1# set group-vpn member ike proposal proposal-name dh-group group
```

```

user@GM1# set group-vpn member ike proposal proposal-name
authentication-algorithm sha1
user@GM1# set group-vpn member ike proposal proposal-name encryption-algorithm
3des-cbc

```

4. Define the IKE policy.

```

[edit security]
user@GM1# set group-vpn member ike policy policy-name mode main
user@GM1# set group-vpn member ike policy policy-name proposals proposal-name
user@GM1# set group-vpn member ike policy policy-name pre-shared-key ascii-text
text

```

5. Set the remote gateways for the IKE gateway group.

```

[edit security]
user@GM1# set group-vpn member ike gateway gateway-group-name ike-policy
policy-name
user@GM1# set group-vpn member ike gateway gateway-group-name server-address
server-IP-address
user@GM1# set group-vpn member ike gateway gateway-group-name local-address
server-facing-interface-IP-address

```



NOTE: To configure a group member to connect to multiple group servers, add the IP address of all the servers to the remote IKE gateway group configuration.

For example,

```

[edit security]
user@GM1# set group-vpn member ike gateway gw-group1 server-address
192.0.2.6
user@GM1# set group-vpn member ike gateway gw-group1 server-address
192.0.2.7

```

6. Configure the group identifier and IKE gateway for the remote gateway group.

```

[edit security]
user@GM1# set group-vpn member ipsec vpn vpn-name ike-gateway
gateway-group-name
user@GM1# set group-vpn member ipsec vpn vpn-name group group-ID
user@GM1# set group-vpn member ipsec vpn vpn-name match-direction output

```

7. In configuration mode, go to the following hierarchy level:

```

[edit]
user@GM1# edit services

```

8. Configure the service set for the remote gateway group.

```

[edit services]
user@GM1# set service-set service-set-name interface-service service-interface
service-interface
user@GM1# set service-set service-set-name ipsec-group-vpn vpn-name

```



NOTE: The service set has to be applied on the interface connecting to the other group member.

For example:

```
[edit interfaces]
user@GM1# set xe-0/3/1 unit 1 family inet service input service-set
gvpn-service-set
user@GM1# set xe-0/3/1 unit 1 family inet service output service-set
gvpn-service-set
```

9. Verify and commit the configuration.

For example:

```
[edit security]
user@GM1# set group-vpn member ike proposal ike-proposal authentication-method
pre-shared-keys
user@GM1# set group-vpn member ike proposal ike-proposal dh-group group2
user@GM1# set group-vpn member ike proposal ike-proposal authentication-algorithm
sha1
user@GM1# set group-vpn member ike proposal ike-proposal encryption-algorithm
3des-cbc
user@GM1# set group-vpn member ike policy ike-policy mode main
user@GM1# set group-vpn member ike policy ike-policy proposals ike-proposal
user@GM1# set group-vpn member ike policy ike-policy pre-shared-key ascii-text
""$9$QEni3/tIRSM87uO87-V4oz36"
user@GM1# set group-vpn member ike gateway gw-group1 ike-policy ike-policy
user@GM1# set group-vpn member ike gateway gw-group1 server-address 192.0.2.6
user@GM1# set group-vpn member ike gateway gw-group1 local-address 203.0.113.1
user@GM1# set group-vpn member ipsec vpn vpn-group1 ike-gateway gw-group1
user@GM1# set group-vpn member ipsec vpn vpn-group1 group 1
user@GM1# set group-vpn member ipsec vpn vpn-group1 match-direction output

[edit services]
user@GM1# set service-set gvpn-service-set interface-service service-interface
ms-4/0/0.1
user@GM1# set service-set gvpn-service-set ipsec-group-vpn vpn-group1

[edit]
user@GM1# commit
commit complete
```

Related Documentation • [Example: Configuring Group VPNs in Group VPNv2 on Routing Devices on page 216](#)

Example: Configuring Group VPNs in Group VPNv2 on Routing Devices



NOTE: Group VPNv2 is the name of the Group VPN technology on MX5, MX10, MX40, MX80, MX240, MX480, and MX960 routers. Group VPNv2 is different from the Group VPN technology implemented on SRX Security Gateways. The term Group VPN is sometimes used in this document to refer to the technology in general, not to the SRX technology.

For more information about Group VPN on SRX Security Gateway devices, see *Group VPNv2 Overview*.

This example shows how to configure Group VPNs in Group VPNv2 to extend the IP Security (IPsec) architecture to support group security associations (GSAs) that are shared by a group of routers.

- [Requirements on page 216](#)
- [Overview on page 216](#)
- [Configuration on page 217](#)
- [Verification on page 226](#)
- [Troubleshooting on page 228](#)

Requirements

This example uses the following hardware and software components:

- Two MX Series 3D Universal Edge Routers with MS-MIC-16G or MS-MPC-PIC line cards
- Reachability to one or more Cisco Group Controllers or Key Servers (GC/KS)
- Junos OS Release 14.1 or later running on the MX Series routers

Before you begin:

1. Configure the routers for network communication.
2. Configure the Cisco GC/KS.
3. Configure the group member device interfaces.

Overview

Starting with Junos OS Release 14.1, MX Series routers with MS-MIC-16G and MS-MPC-PIC line cards provide the Group VPNv2 member functionality support with one or more Cisco Group Controllers or Key Servers (GC/KS). The group members can connect to a maximum of four Cisco GC/KSs with minimum interoperability with the cooperative servers.

This feature also provides system logging support for Group VPNv2 functionality, and routing instance support for both control and data traffic.

Topology

In [Figure 17 on page 217](#), a Group VPN is configured between a Cisco group server, GC/KS – and two group members, GM1 and GM2. The group members are connected to host devices.

In [Figure 18 on page 217](#), a Group VPN is configured between GM1 and GM2, and GC/KS1 and GC/KS2 are the primary and secondary group servers, respectively.

Figure 17: Group VPN with Single GC/KS

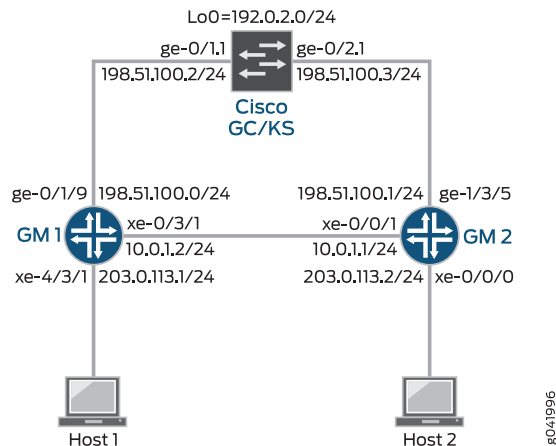
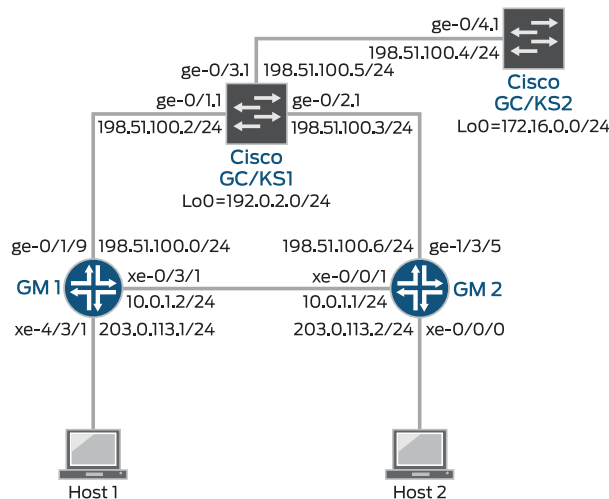


Figure 18: Group VPN with Multiple GC/KS



Configuration

- [Configuring Group VPNv2 with a Single GC/KS on page 218](#)
- [Configuring Group VPNv2 with Multiple GC/KS on page 222](#)

Configuring Group VPNv2 with a Single GC/KS

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then **commit** the configuration.

```

GM1  set interfaces ms-4/0/0 unit 1 family inet
      set interfaces ge-0/1/9 vlan-tagging
      set interfaces ge-0/1/9 unit 1 vlan-id 11
      set interfaces ge-0/1/9 unit 1 family inet address 198.51.100.1/24
      set interfaces xe-0/3/1 vlan-tagging
      set interfaces xe-0/3/1 unit 1 vlan-id 1
      set interfaces xe-0/3/1 unit 1 family inet service input service-set gvpn-service-set
      set interfaces xe-0/3/1 unit 1 family inet service output service-set gvpn-service-set
      set interfaces xe-0/3/1 unit 1 family inet address 10.0.1.2/24
      set interfaces xe-4/3/1 unit 0 family inet address 203.0.113.1/24
      set routing-options static route 192.0.2.0/24 next-hop 198.51.100.2
      set routing-options static route 203.0.113.3/24 next-hop 10.0.1.1
      set security group-vpn member ike proposal ike-proposal authentication-method
        pre-shared-keys
      set security group-vpn member ike proposal ike-proposal dh-group group2
      set security group-vpn member ike proposal ike-proposal authentication-algorithm sha1
      set security group-vpn member ike proposal ike-proposal encryption-algorithm 3des-cbc
      set security group-vpn member ike policy ike-policy mode main
      set security group-vpn member ike policy ike-policy proposals ike-proposal
      set security group-vpn member ike policy ike-policy pre-shared-key ascii-text
        ""$9$QEni3/t1RSM87uO87-V4oz36"
      set security group-vpn member ike gateway gw-group1 ike-policy ike-policy
      set security group-vpn member ike gateway gw-group1 server-address 192.0.2.0
      set security group-vpn member ike gateway gw-group1 local-address 198.51.100.1
      set security group-vpn member ipsec vpn vpn-group1 ike-gateway gw-group1
      set security group-vpn member ipsec vpn vpn-group1 group 1
      set security group-vpn member ipsec vpn vpn-group1 match-direction output
      set services service-set gvpn-service-set interface-service service-interface ms-4/0/0.1
      set services service-set gvpn-service-set ipsec-group-vpn vpn-group1

GM2  set interfaces ms-0/2/0 unit 1 family inet
      set interfaces xe-0/0/0 unit 0 family inet address 203.0.113.2/24
      set interfaces xe-0/1/1 vlan-tagging
      set interfaces xe-0/1/1 unit 1 vlan-id 1
      set interfaces xe-0/1/1 unit 1 family inet service input service-set gvpn-service-set
      set interfaces xe-0/1/1 unit 1 family inet service output service-set gvpn-service-set
      set interfaces xe-0/1/1 unit 1 family inet address 10.0.1.1/24
      set interfaces ge-1/3/5 vlan-tagging
      set interfaces ge-1/3/5 unit 1 vlan-id 11
      set interfaces ge-1/3/5 unit 1 family inet address 198.51.100.1/24
      set routing-options static route 192.0.2.0/24 next-hop 198.51.100.3
      set routing-options static route 203.0.113.4/24 next-hop 10.0.1.2
      set security group-vpn member ike proposal ike-proposal authentication-method
        pre-shared-keys
      set security group-vpn member ike proposal ike-proposal dh-group group2
      set security group-vpn member ike proposal ike-proposal authentication-algorithm sha1
      set security group-vpn member ike proposal ike-proposal encryption-algorithm 3des-cbc
      set security group-vpn member ike policy ike-policy mode main

```

```

set security group-vpn member ike policy ike-policy proposals ike-proposal
set security group-vpn member ike policy ike-policy pre-shared-key ascii-text
  "$9$QEni3/tIRSM87uO87-V4oz36"
set security group-vpn member ike gateway gw-group1 ike-policy ike-policy
set security group-vpn member ike gateway gw-group1 server-address 192.0.2.0
set security group-vpn member ike gateway gw-group1 local-address 198.51.100.1
set security group-vpn member ipsec vpn vpn-group1 ike-gateway gw-group1
set security group-vpn member ipsec vpn vpn-group1 group 1
set security group-vpn member ipsec vpn vpn-group1 match-direction output
set services service-set gvpn-service-set interface-service service-interface ms-0/2/0.1
set services service-set gvpn-service-set ipsec-group-vpn vpn-group1

```

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 GM1:

1. Configure the Router GM1 interfaces.

```
[edit interfaces]
```

```
user@GM1# set ms-4/0/0 unit 1 family inet
```

```
user@GM1# set ge-0/1/9 vlan-tagging
```

```
user@GM1# set ge-0/1/9 unit 1 vlan-id 11
```

```
user@GM1# set ge-0/1/9 unit 1 family inet address 198.51.100.1/24
```

```
user@GM1# set xe-0/3/1 vlan-tagging
```

```
user@GM1# set xe-0/3/1 unit 1 vlan-id 1
```

```
user@GM1# set xe-0/3/1 unit 1 family inet service input service-set gvpn-service-set
```

```
user@GM1# set xe-0/3/1 unit 1 family inet service output service-set gvpn-service-set
```

```
user@GM1# set xe-0/3/1 unit 1 family inet address 10.0.1.2/24
```

```
user@GM1# set interfaces xe-4/3/1 unit 0 family inet address 203.0.113.1/24
```

2. Configure static routes to reach the group server and member 2.

```
[edit routing-options]
```

```
user@GM1# set static route 192.0.2.0/24 next-hop 198.51.100.2
```

```
user@GM1# set static route 203.0.113.3/24 next-hop 10.0.1.1
```

3. Define the IKE proposal.

```
[edit security]
```

```
user@GM1# set group-vpn member ike proposal ike-proposal
```

4. Configure the Phase 1 SA for ike-proposal.

```
[edit security]
```

```
user@GM1# set group-vpn member ike proposal ike-proposal authentication-method
pre-shared-keys
```

```
user@GM1# set group-vpn member ike proposal ike-proposal dh-group group2
```

```
user@GM1# set group-vpn member ike proposal ike-proposal
```

```
authentication-algorithm sha1
```

```
user@GM1# set group-vpn member ike proposal ike-proposal encryption-algorithm
3des-cbc
```

5. Define the IKE policy.

```
[edit security]
user@GM1# set group-vpn member ike policy ike-policy mode main
user@GM1# set group-vpn member ike policy ike-policy proposals ike-proposal
user@GM1# set group-vpn member ike policy ike-policy pre-shared-key ascii-text
    ""$9$QEni3/t1RSM87uO87-V4oz36"
```

6. Set the remote gateways for gw-group1.

```
[edit security]
user@GM1# set group-vpn member ike gateway gw-group1 ike-policy ike-policy
user@GM1# set group-vpn member ike gateway gw-group1 server-address 192.0.2.0
user@GM1# set group-vpn member ike gateway gw-group1 local-address 198.51.100.1
```

7. Configure the group identifier and IKE gateway for gw-group1.

```
[edit security]
user@GM1# set group-vpn member ipsec vpn vpn-group1 ike-gateway gw-group1
user@GM1# set group-vpn member ipsec vpn vpn-group1 group 1
user@GM1# set group-vpn member ipsec vpn vpn-group1 match-direction output
```

8. Configure the service set for gw-group1.

```
[edit services]
user@GM1# set service-set gvpn-service-set interface-service service-interface
    ms-4/0/0.1
user@GM1# set service-set gvpn-service-set ipsec-group-vpn vpn-group1
```

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

```
GM1 user@GM1# show interfaces
ge-0/1/9 {
  vlan-tagging;
  unit 1 {
    vlan-id 11;
    family inet {
      address 198.51.100.1/24;
    }
  }
}
xe-0/3/1 {
  vlan-tagging;
  unit 1 {
    vlan-id 1;
    family inet {
      service {
        input {
          service-set gvpn-service-set;
        }
        output {
          service-set gvpn-service-set;
        }
      }
    }
  }
  address 10.0.1.2/24;
```



```

    }
  }
}
ms-4/0/0 {
  unit 1 {
    family inet;
  }
}
xe-4/3/1 {
  unit 0 {
    family inet {
      address 203.0.113.1/24;
    }
  }
}
}

user@GM1# show routing-options
static {
  route 192.0.2.0/24 next-hop 198.51.100.2;
  route 203.0.113.3/24 next-hop 10.0.1.1;
}

user@GM1# show security
group-vpn {
  member {
    ike {
      proposal ike-proposal {
        authentication-method pre-shared-keys;
        dh-group group2;
        authentication-algorithm sha1;
        encryption-algorithm 3des-cbc;
      }
      policy ike-policy {
        mode main;
        pre-shared-key ascii-text ""$9$QEni3/t1RSM87uO87-V4oz36"; ## SECRET-DATA
        proposals ike-proposal;
      }
      gateway gw-group1 {
        ike-policy ike-policy;
        server-address 192.0.2.0;
        local-address 198.51.100.1;
      }
    }
    ipsec {
      vpn vpn-group1 {
        ike-gateway gw-group1;
        group 1;
        match-direction output;
      }
    }
  }
}

user@GM1# show services
service-set gvpn-service-set {
  interface-service {

```

```

        service-interface ms-4/0/0.1;
    }
    ipsec-group-vpn vpn-group1;
}

```

Configuring Group VPNv2 with Multiple GC/KS

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then **commit** the configuration.

```

GM1  set interfaces ms-4/0/0 unit 1 family inet
      set interfaces ge-0/1/9 vlan-tagging
      set interfaces ge-0/1/9 unit 1 vlan-id 11
      set interfaces ge-0/1/9 unit 1 family inet address 198.51.100.1/24
      set interfaces xe-0/3/1 vlan-tagging
      set interfaces xe-0/3/1 unit 1 vlan-id 1
      set interfaces xe-0/3/1 unit 1 family inet service input service-set gvpn-service-set
      set interfaces xe-0/3/1 unit 1 family inet service output service-set gvpn-service-set
      set interfaces xe-0/3/1 unit 1 family inet address 10.0.1.2/24
      set interfaces xe-4/3/1 unit 0 family inet address 203.0.113.1/24
      set routing-options static route 192.0.2.0/24 next-hop 198.51.100.2
      set routing-options static route 203.0.113.3/24 next-hop 10.0.1.1
      set security group-vpn member ike proposal ike-proposal authentication-method
        pre-shared-keys
      set security group-vpn member ike proposal ike-proposal dh-group group2
      set security group-vpn member ike proposal ike-proposal authentication-algorithm sha1
      set security group-vpn member ike proposal ike-proposal encryption-algorithm 3des-cbc
      set security group-vpn member ike policy ike-policy mode main
      set security group-vpn member ike policy ike-policy proposals ike-proposal
      set security group-vpn member ike policy ike-policy pre-shared-key ascii-text
        ""$9$QEni3/t1RSM87uO87-V4oz36"
      set security group-vpn member ike gateway gw-group1 ike-policy ike-policy
      set security group-vpn member ike gateway gw-group1 server-address 192.0.2.0
      set security group-vpn member ike gateway gw-group1 server-address 192.0.2.1
      set security group-vpn member ike gateway gw-group1 local-address 198.51.100.1
      set security group-vpn member ipsec vpn vpn-group1 ike-gateway gw-group1
      set security group-vpn member ipsec vpn vpn-group1 group 1
      set security group-vpn member ipsec vpn vpn-group1 match-direction output
      set services service-set gvpn-service-set interface-service service-interface ms-4/0/0.1
      set services service-set gvpn-service-set ipsec-group-vpn vpn-group1

GM2  set interfaces ms-0/2/0 unit 1 family inet
      set interfaces xe-0/0/0 unit 0 family inet address 203.0.113.2/24
      set interfaces xe-0/1/1 vlan-tagging
      set interfaces xe-0/1/1 unit 1 vlan-id 1
      set interfaces xe-0/1/1 unit 1 family inet service input service-set gvpn-service-set
      set interfaces xe-0/1/1 unit 1 family inet service output service-set gvpn-service-set
      set interfaces xe-0/1/1 unit 1 family inet address 10.0.1.1/24
      set interfaces ge-1/3/5 vlan-tagging
      set interfaces ge-1/3/5 unit 1 vlan-id 11
      set interfaces ge-1/3/5 unit 1 family inet address 198.51.100.1/24
      set routing-options static route 192.0.2.0/24 next-hop 198.51.100.3
      set routing-options static route 203.0.113.4/24 next-hop 10.0.1.2

```

```

set security group-vpn member ike proposal ike-proposal authentication-method
pre-shared-keys
set security group-vpn member ike proposal ike-proposal dh-group group2
set security group-vpn member ike proposal ike-proposal authentication-algorithm sha1
set security group-vpn member ike proposal ike-proposal encryption-algorithm 3des-cbc
set security group-vpn member ike policy ike-policy mode main
set security group-vpn member ike policy ike-policy proposals ike-proposal
set security group-vpn member ike policy ike-policy pre-shared-key ascii-text
    "$9$QEni3/tIRSM87uO87-V4oz36"
set security group-vpn member ike gateway gw-group1 ike-policy ike-policy
set security group-vpn member ike gateway gw-group1 server-address 192.0.2.0
set security group-vpn member ike gateway gw-group1 server-address 192.0.2.1
set security group-vpn member ike gateway gw-group1 local-address 198.51.100.1
set security group-vpn member ipsec vpn vpn-group1 ike-gateway gw-group1
set security group-vpn member ipsec vpn vpn-group1 group 1
set security group-vpn member ipsec vpn vpn-group1 match-direction output
set services service-set gvpn-service-set interface-service service-interface ms-0/2/0.1
set services service-set gvpn-service-set ipsec-group-vpn vpn-group1

```

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 GM1:

1. Configure the Router GM1 interfaces.

[edit interfaces]

```
user@GM1# set ms-4/0/0 unit 1 family inet
```

```
user@GM1# set ge-0/1/9 vlan-tagging
```

```
user@GM1# set ge-0/1/9 unit 1 vlan-id 11
```

```
user@GM1# set ge-0/1/9 unit 1 family inet address 198.51.100.1/24
```

```
user@GM1# set xe-0/3/1 vlan-tagging
```

```
user@GM1# set xe-0/3/1 unit 1 vlan-id 1
```

```
user@GM1# set xe-0/3/1 unit 1 family inet service input service-set gvpn-service-set
```

```
user@GM1# set xe-0/3/1 unit 1 family inet service output service-set gvpn-service-set
```

```
user@GM1# set xe-0/3/1 unit 1 family inet address 10.0.1.2/24
```

```
user@GM1# set xe-4/3/1 unit 0 family inet address 203.0.113.1/24
```

2. Configure static routes to reach the group server and member 2.

[edit routing-options]

```
user@GM1# set static route 192.0.2.0/24 next-hop 198.51.100.2
```

```
user@GM1# set static route 203.0.113.3/24 next-hop 10.0.1.1
```

3. Define the IKE proposal.

[edit security]

```
user@GM1# set group-vpn member ike proposal ike-proposal
```

4. Configure the Phase 1 SA for ike-proposal.

[edit security]

```

user@GM1# set group-vpn member ike proposal ike-proposal authentication-method
pre-shared-keys
user@GM1# set group-vpn member ike proposal ike-proposal dh-group group2
user@GM1# set group-vpn member ike proposal ike-proposal
authentication-algorithm sha1
user@GM1# set group-vpn member ike proposal ike-proposal encryption-algorithm
3des-cbc

```

5. Define the IKE policy.

```

[edit security]
user@GM1# set group-vpn member ike policy ike-policy mode main
user@GM1# set group-vpn member ike policy ike-policy proposals ike-proposal
user@GM1# set group-vpn member ike policy ike-policy pre-shared-key ascii-text
""$9$QEni3/t1RSM87uO87-V4oz36"

```

6. Set the remote gateways for gw-group1.

```

[edit security]
user@GM1# set group-vpn member ike gateway gw-group1 ike-policy ike-policy
user@GM1# set group-vpn member ike gateway gw-group1 server-address 192.0.2.0
user@GM1# set group-vpn member ike gateway gw-group1 server-address 192.0.2.1
user@GM1# set group-vpn member ike gateway gw-group1 local-address 198.51.100.1

```

7. Configure the group identifier and IKE gateway for gw-group1.

```

[edit security]
user@GM1# set group-vpn member ipsec vpn vpn-group1 ike-gateway gw-group1
user@GM1# set group-vpn member ipsec vpn vpn-group1 group 1
user@GM1# set group-vpn member ipsec vpn vpn-group1 match-direction output

```

8. Configure the service set for gw-group1.

```

[edit services]
user@GM1# set service-set gvpn-service-set interface-service service-interface
ms-4/0/0.1
user@GM1# set service-set gvpn-service-set ipsec-group-vpn vpn-group1

```

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

```

GM1 user@GM1# show interfaces
ge-0/1/9 {
  vlan-tagging;
  unit 1 {
    vlan-id 11;
    family inet {
      address 198.51.100.1/24;
    }
  }
}
xe-0/3/1 {
  vlan-tagging;
  unit 1 {
    vlan-id 1;
    family inet {

```

```

    service {
        input {
            service-set gvpn-service-set;
        }
        output {
            service-set gvpn-service-set;
        }
    }
    address 10.0.1.2/24;
}
}
ms-4/0/0 {
    unit 1 {
        family inet;
    }
}
xe-4/3/1 {
    unit 0 {
        family inet {
            address 203.0.113.1/24;
        }
    }
}
}

```

```
user@GM1# show routing-options
```

```
static {
    route 192.0.2.0/24 next-hop 198.51.100.2;
    route 203.0.113.3/24 next-hop 10.0.1.1;
}

```

```
user@GM1# show security
```

```
group-vpn {
    member {
        ike {
            proposal ike-proposal {
                authentication-method pre-shared-keys;
                dh-group group2;
                authentication-algorithm sha1;
                encryption-algorithm 3des-cbc;
            }
            policy ike-policy {
                mode main;
                pre-shared-key ascii-text ""$9$QEni3/tIRSM87uO87-V4oz36""; ## SECRET-DATA
                proposals ike-proposal;
            }
            gateway gw-group1 {
                ike-policy ike-policy;
                server-address [ 192.0.2.0 192.0.2.1 ];
                local-address 198.51.100.1;
            }
        }
    }
    ipsec {
        vpn vpn-group1 {
            ike-gateway gw-group1;
            group 1;
        }
    }
}

```

```
        match-direction output;
    }
}
}
}

user@GM1# show services
service-set gvpn-service-set {
    interface-service {
        service-interface ms-4/0/0.1;
    }
    ipsec-group-vpn vpn-group1;
}
```

Verification

Confirm that the configuration is working properly.

- [Verifying the Group Member IKE SA on page 226](#)
- [Verifying the Group Member IPsec SA on page 227](#)
- [Verifying the Group Member IPsec Statistics on page 227](#)

Verifying the Group Member IKE SA

Purpose Verify the IKE SAs on Router GM1.

Action From operational mode, run the **show security group-vpn member ike security-associations detail** command.

```
user@GM1> show security group-vpn member ike security-associations detail
IKE peer 192.0.2.0, Index 2994970, Gateway Name: gw-group1
  Role: Initiator, State: UP
  Initiator cookie: 7fad16089a123bcd, Responder cookie: 536b33ffe89799de
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local:198.51.100.1:848, Remote:192.0.2.0:848
  Lifetime: Expires in 175 seconds
  Peer ike-id: 192.0.2.0
  Xauth user-name: not available
  Xauth assigned IP: 0.0.0.0
  Algorithms:
    Authentication      : hmac-sha1-96
    Encryption          : 3des-cbc
    Pseudo random function: hmac-sha1
    Diffie-Hellman group : DH-group-2
  Traffic statistics:
    Input bytes  :          752
    Output bytes :          716
    Input packets:           5
    Output packets:          5
  Flags: IKE SA is created
  IPSec security associations: 0 created, 0 deleted
  Phase 2 negotiations in progress: 0
```

Meaning Router GM1 has established the IKE SA with the GC/KS for the group.

Verifying the Group Member IPsec SA

Purpose Verify the IPsec SAs on Router GM1.

Action From operational mode, run the **show security group-vpn member ipsec security-associations detail** command.

```
user@GM1> show security group-vpn member ipsec security-associations detail
Virtual-system: root Group VPN Name: vpn-group1
  Local Gateway: 198.51.100.1, GDOI Server: 192.0.2.0
  Group Id: 1
  Rule Match Direction: output, Tunnel-MTU: 1500
  Routing Instance: default
  DF-bit: clear
  Stats:
    Pull Succeeded           : 18
    Pull Failed              : 0
    Pull Timeout             : 0
    Pull Aborted             : 0
    Server Failover          : 0
    Delete Received          : 0
    Exceed Maximum Keys(4)   : 0
    Exceed Maximum Policies(1): 0
    Unsupported Algo         : 0
  Flags:
    Rekey Needed: no

  List of policies received from server:
  Tunnel-id: 10001
    Source IP: ipv4_subnet(any:0,[0..7]=203.0.113.4/24)
    Destination IP: ipv4_subnet(any:0,[0..7]=203.0.113.3/24)

    Direction: bi-directional, SPI: e1c117c7
    Protocol: ESP, Authentication: sha1, Encryption: 3des
    Hard lifetime: Expires in 2526 seconds
    Lifesize Remaining: Unlimited
    Soft lifetime: Expires in 2366 seconds
    Mode: Tunnel, Type: Group VPN, State: installed
    Anti-replay service: N/A
```

Meaning Router GM1 has established the IPsec SA with the GC/KS.

Verifying the Group Member IPsec Statistics

Purpose Verify the IPsec statistics on Router GM1.

Action From operational mode, run the **show security group-vpn member ipsec statistics** command.

```
user@GM1> show security group-vpn member ipsec statistics
PIC: ms-0/2/0, Service set: gvpn-service-set
```

```
ESP Statistics:
  Encrypted bytes:          264
  Decrypted bytes:         264
  Encrypted packets:        3
  Decrypted packets:        3
AH Statistics:
  Input bytes:              0
  Output bytes:             0
  Input packets:            0
  Output packets:           0
Errors:
  AH authentication failures: 0
  ESP authentication failures: 0
  ESP decryption failures:    0
  Bad headers: 0, Bad trailers: 0
  Replay before window drops: 0, Replayed pkts: 0
  IP integrity errors: 0, Exceeds tunnel MTU: 0
  Rule lookup failures: 0, No SA errors: 0
  Flow errors: 0, Misc errors: 0
```

Meaning **ESP Statistics** shows that packet flows have been encrypted and decrypted between the group members. Router GM1 has encrypted 3 packets and has received 3 decrypted packets from Router GM2.

Troubleshooting

To troubleshoot the Group VPNv2 configuration, see:

- [Negotiating the IKE SA on page 228](#)
- [Establishing the IKE SA on page 229](#)
- [Downloading the GDOI IPsec SA on page 229](#)
- [Traffic Encryption and Decryption on page 230](#)
- [Troubleshooting System Log Messages on page 230](#)

Negotiating the IKE SA

Problem The IKE SA negotiation is not triggered on the group member.

The output of the **show ike** and **show security group-vpn member ike security-associations** commands does not display the IKE negotiations.

Solution To troubleshoot the IKE negotiation issue:

1. Check if the service interface status is up.

Use **show interfaces terse | match ms** to check if the MS interface is down. An MS interface goes down when the PIC is rebooting.

2. Look for **Ignore gvpn vpn_name** since it is inactive in the log file `/var/log/gkmd`.

Check if the Group VPN is referenced by any service set in the configuration.

- a. Enable **security group-vpn member ike traceoptions**.
- b. Look for the following system log messages in the trace log file:
 - Dec 2 16:09:54 GVPN:iked_pm_gvpn_trigger called for gvpn200
 - Dec 2 16:09:54 GVPN:PM NULL for gvpn gvpn200
 - Dec 2 16:09:54 GVPN:Ignore gvpn gvpn200 since it is inactive

This means either the service set is inactive or the service interface is down.

Establishing the IKE SA

Problem The IKE SA is not getting established with the GC/KS.

In this scenario, the IKE SA state is down in the **show security group-vpn member ike security-associations** command output:

```
user@GM1> show security group-vpn member ike security-associations
Index   State Initiator cookie Responder cookie Mode Remote Address
-----
          5295626 DOWN 2d47c125d2a9805e 0000000000000000 Main
192.0.2.3
```

Solution To troubleshoot the IKE SA issue:

1. Check if the server address configured under **[edit security group-vpn member ike gateway]** is the correct one and is reachable.
2. Use the **ping** command between the remote devices to check network connectivity.
3. Check if the local address in the **group-vpn** configuration is also a configured address on any of the physical interfaces in the configuration.
4. Check if the IKE proposals match between the group member and the GC/KS.

If there is a misconfiguration on the IKE SA negotiation, then do the following:

- a. Enable **security group-vpn member ike traceoption**.
- b. Look for the following message in the trace log file:


```
Dec 2 15:39:54 ikev2_fb_negotiation_done_isakmp: Entered IKE error code No proposal
chosen (14), IKE SA 8dd7000 (neg 8dda800).
```
5. Look for a **No proposal chosen** error in the log file `/var/log/gkmd`.

Downloading the GDOI IPsec SA

Problem The GDOI IPsec SAs are not downloaded from the GC/KS.

In this scenario, the GDOI **groupkey-pull** with the configured GC/KS fails, and the **show security group-vpn member ipsec sa** command output does not display anything.

Solution To troubleshoot the GDOI IPsec SA issue:

1. Check if the IKE SA has been established with the GC/KS.
2. Check if the group ID configured on the GC/KS and the group member match.
3. Look for any group SA installation failures or other failures in the log file `/var/log/gkmd`.

Look for the following syslog messages to confirm use of an unsupported GDOI SA algorithm:

- Dec 2 15:32:49 simpleman gkmd[1701]: Failed to install SA because of unsupported algo(encr: 3des-cbc, auth : (null)) for SPI 0x6645cdb5 from server 172.16.0.1
- Dec 2 15:32:49 simpleman gkmd[1701]: Member registration failed with key server 172.16.0.1 for group vpn gvpn200, reason SA unusable

Look for the following syslog messages to confirm use of unsupported GDOI policies:

- Dec 2 15:34:34 simpleman gkmd[1701]: Failed to install SA because of too many(2) policies for SPI 0x6951550c from server 172.16.0.1
- Dec 2 15:34:34 simpleman gkmd[1701]: Member registration failed with key server 172.16.0.1 for group vpn gvpn200, reason SA unusable

Traffic Encryption and Decryption

Problem The CLI shows IPsec SAs as installed, but traffic does not go through the SAs.

In this scenario, traffic matching the rules received from the server fails to get encrypted or decrypted. The **show security group-vpn member ipsec statistics** command output displays a zero value for encrypt and decrypt packet count.

Solution Look for **Rule lookup failures** counter in the error section of the CLI output.

Troubleshooting System Log Messages

Problem System log messages are generated to record the different Group VPNv2 events.

Solution To interpret the system log messages, refer to the following:

- Dec 2 15:29:10 simpleman gkmd[1701]: Member registration succeeded with key server 172.16.0.1 for group vpn gvpn200—GDOI pull was successful.
- Dec 2 15:21:18 simpleman gkmd[1701]: Member registration failed with key server 172.16.0.1 for group vpn gvpn200, reason Timed out—GDOI pull failed.
- Dec 2 15:34:34 simpleman gkmd[1701]: Failed to install SA because of too many(2) policies for SPI 0x6951550c from server 172.16.0.1—GDOI SA installation failed because of too many policies.

- Dec 2 15:21:18 simpleman gkmd[1701]: Server 172.16.0.1 is unreachable for group vpn gvpn200—Single GC/KS failed (Non-COOP).
- Dec 2 15:51:49 simpleman gkmd[1701]: Current key server 172.16.0.1 is unreachable and will try registering with next Key Server 110.1.1.2 for group vpn gvpn200—Particular GC/KS is not responding (COOP).
- Dec 2 15:56:24 simpleman gkmd[1701]: All servers are unreachable for group vpn gvpn200—None of the GC/KS are responding (COOP).
- Dec 2 16:01:43 simpleman gkmd[1701]: Member re-registering with Key Server 172.16.0.1 for group-vpn gvpn200—Member re-registration with the GC/KS.
- Dec 2 16:01:43 simpleman gkmd[1701]: Creating TEK with SPI 0xb35200ac tunnel_id 10001 for group vpn gvpn200—GDOI SA TEK creation was successful.
- Dec 2 16:29:01 simpleman gkmd[1701]: Deleting TEK with SPI 0x6dba2a76 tunnel_id 10001 for group vpn gvpn200 and reason cleared from CLI—GDOI SA TEK destroy was successful with reason.

Different reasons for the GDOI SA TEK destroy are as follows:

- Cleared from CLI
- Hard lifetime expired
- Too many TEKs
- Configuration change
- SA install error
- Stale SA
- Interface down

- Related Documentation**
- *Use Case for Configuring Group VPNv2*
 - [Group VPNv2 Overview on page 193](#)

PART 4

Configuring Ethernet VPNs

- [Overview on page 235](#)
- [Configuring Routing Instances for EVPN on page 239](#)
- [Configuring EVPN Multihoming on page 245](#)
- [Configuring Integrated Bridging and Routing Using EVPNs on page 297](#)
- [Configuring EVPN with Support for Virtual Switch on page 325](#)

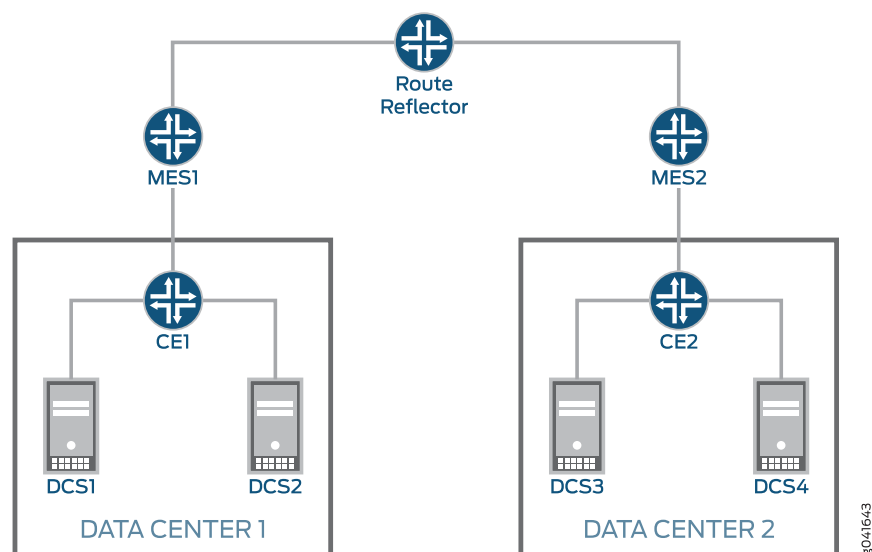
Overview

- [EVPN Overview on page 235](#)
- [Supported EVPN Standards on page 236](#)

EVPN Overview

An Ethernet VPN (EVPN) enables you to connect dispersed customer sites using a Layer 2 virtual bridge. As with other types of VPNs, an EVPN consists of customer edge (CE) devices (host, router, or switch) connected to provider edge (PE) routers. The PE routers can include an MPLS edge switch (MES) that acts at the edge of the MPLS infrastructure. Either an MX Series 3D Universal Edge Router or a standalone switch can be configured to act as an MES. You can deploy multiple EVPNs within a service provider network, each providing network connectivity to a customer while ensuring that the traffic sharing on that network remains private. [Figure 19 on page 235](#) illustrates a typical EVPN deployment. Traffic from Data Center 1 is transported over the service provider's network through MES1 to MES2 and then onto Data Center 2. DCS1, DCS2, DCS3, and DCS4 are the data center switches.

Figure 19: EVPN Connecting Data Center 1 and Data Center 2



The MESs are interconnected within the service provider's network using label-switched paths (LSPs). The MPLS infrastructure allows you to take advantage of the MPLS functionality provided by the Junos OS, including fast reroute, node and link protection, and standby secondary paths. For EVPNs, learning between MESs takes place in the control plane rather than in the data plane (as is the case with traditional network bridging). The control plane provides greater control over the learning process, allowing you to restrict which devices discover information about the network. You can also apply policies on the MESs, allowing you to carefully control how network information is distributed and processed. EVPNs utilize the BGP control plane infrastructure, providing greater scale and the ability to isolate groups of devices (hosts, servers, virtual machines, and so on) from each other.

The MESs attach an MPLS label to each MAC address learned from the CE devices. This label and MAC address combination is advertised to the other MESs in the control plane. Control plane learning enables load balancing and improves convergence times in the event of certain types of network failures. The learning process between the MESs and the CE devices is completed using the method best suited to each CE device (data plane learning, IEEE 802.1, LLDP, 802.1aq, and so on).

The policy attributes of an EVPN are similar to an IP VPN (for example, Layer 3 VPNs). Each EVPN routing instance requires that you configure a route distinguisher (RD) and one or more route targets (RTs). A CE device attaches to an EVPN routing instance on an MES through an Ethernet interface that might be configured for one or more VLANs.

The following features are available for EVPNs:

- Ethernet connectivity between data centers spanning metropolitan area networks (MANs) and WANs
- One VLAN for each MAC VPN
- Automatic RDs
- Dual-homed EVPN connection with active/standby multihoming

The following features are not supported for EVPNs:

- Active/active multihoming

**Related
Documentation**

- [Supported EVPN Standards on page 236](#)
- [EVPN Overview on page 235](#)

Supported EVPN Standards

Junos OS supports the following RFCs and Internet drafts that define standards for EVPNs:

- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*
- RFC 7432, *BGP MPLS-Based Ethernet VPN*

The following features are not supported:

- Automatic derivation of Ethernet segment (ES) values. Only static ES configurations are supported.
- Host proxy ARP.
- MAC mobility extended community.
- VLAN bundle service interface.

**Related
Documentation**

- [EVPN Overview on page 235](#)
- *Accessing Standards Documents on the Internet*

Configuring Routing Instances for EVPN

- [Configuring EVPN Routing Instances on page 239](#)
- [Tracing EVPN Traffic and Operations on page 242](#)

Configuring EVPN Routing Instances

To configure an EVPN routing instance, complete the following configuration on the PE router (or on the MPLS edge switch) within the EVPN service provider's network:

1. Configure the EVPN routing instance name using the **routing-instances** statement at the **[edit]** hierarchy level:

```
routing-instances routing-instance-name {...}
```

2. Configure the **evpn** option for the **instance-type** statement at the **[edit routing-instances *routing-instance-name*]** hierarchy level:

```
instance-type evpn;
```



NOTE: For MX Series devices and EX Series switches, you can include multiple IFLs of an Ethernet segment identifier (ESI) across different bridge-domains of an EVPN routing instance in all-active mode. However, you cannot include multiple IFLs of the same ESI within the same bridge-domain.

3. Configure the interfaces for handling EVPN traffic between the MES and the CE device using the **interface** statement at the **[edit routing-instances *routing-instance-name*]** hierarchy level:

```
interface interface-name;
```

4. Configure a VLAN identifier for the EVPN routing instance using the **vlan-id** statement at the **[edit routing-instances *routing-instance-name*]** hierarchy level:

```
vlan-id (vlan-id | all | none);
```

5. Configure a route distinguisher on a PE router by including the **route-distinguisher** statement:

```
route-distinguisher (as-number:number | ip-address:number);
```

Each routing instance that you configure on a PE router must have a unique route distinguisher associated with it. VPN routing instances need a route distinguisher to help BGP to distinguish between potentially identical network layer reachability information (NLRI) messages received from different VPNs. If you configure different VPN routing instances with the same route distinguisher, the commit fails.

For a list of the hierarchy levels at which you can include this statement, see the statement summary for this statement.

The route distinguisher is a 6-byte value that you can specify in one of the following formats:

- **as-number:number**, where **as-number** is an autonomous system (AS) number (a 2-byte value) and **number** is any 4-byte value. The AS number can be in the range 1 through 65,535. We recommend that you use an Internet Assigned Numbers Authority (IANA)-assigned, nonprivate AS number, preferably the Internet service provider's (ISP's) own or the customer's own AS number.
 - **ip-address:number**, where **ip-address** is an IP address (a 4-byte value) and **number** is any 2-byte value. The IP address can be any globally unique unicast address. We recommend that you use the address that you configure in the **router-id** statement, which is a nonprivate address in your assigned prefix range.
6. Configure either import and export policies for the EVPN routing table, or configure the default policies using the **vrf-target** statement configured at the **[edit routing-instances routing-instance-name]** hierarchy level.

See [“Configuring Policies for the VRF Table on PE Routers in VPNs” on page 25](#).
 7. Configure each EVPN interface for the EVPN routing instance:



NOTE: When adding a trunk port with dual tags to an EVPN and MPLS routing instance, or an EVPN and VXLAN routing instance, the CLI commit check configuration fails and generates an error. To avoid configuration check errors, use sub-interface style interface configuration with dual tags for the routing instances.

- a. Configure each interface using the **interface** statement at the **[edit routing-instances routing-instance-name protocols evpn]** hierarchy level.
- b. Configure interface encapsulation for the CE facing interfaces at the **[edit interfaces interface-name encapsulation]** hierarchy level. Supported encapsulations, are: **(ethernet-bridge | vlan-bridge | extended-vlan-bridge)**
- c. (Optional) Allow the EVPN to establish a connection to the CE device even if the CE device interface encapsulation and the EVPN interface encapsulations do not match by including the **ignore-encapsulation-mismatch** statement at the **[edit routing-instances routing-instance-name protocols evpn interface interface-name]** hierarchy level.
- d. (Optional) Specify a static MAC address for a logical interface in a bridge domain using the **static-mac** statement at the **[edit routing-instances routing-instance-name protocols evpn interface interface-name]** hierarchy level.

8. Specify the maximum number of media access control (MAC) addresses that can be learned by the EVPN routing instance by including the [interface-mac-limit](#) statement.

You can configure the same limit for all interfaces configured for a routing instance by including this statement at the **[edit routing-instances *routing-instance-name* protocols evpn]** hierarchy level. You can also configure a limit for a specific interface by including this statement at the **[edit routing-instances *routing-instance-name* protocols evpn interface *interface-name*]** hierarchy level.

By default, packets with new source MAC addresses are forwarded after the MAC address limit is reached. You can alter this behavior by including the [packet-action drop](#) statement at either the **[edit routing-instances *routing-instance-name* protocols evpn interface-mac-limit]** or the **[edit routing-instances *routing-instance-name* protocols evpn interface *interface-name*]** hierarchy level. If you configure this statement, packets from new source MAC addresses are dropped once the configured MAC address limit is reached.

9. Specify the MPLS label allocation setting for the EVPN by including the [label-allocation](#) statement with the **per-instance** option at the **[edit routing-instances *routing-instance-name* protocols evpn]** hierarchy level.

If you configure this statement, one MPLS label is allocated for the specified EVPN routing instance.

10. Enable MAC accounting for the EVPN by including the [mac-statistics](#) statement at the **[edit routing-instances *routing-instance-name* protocols evpn]** hierarchy level.
11. Specify the number of addresses that can be stored in the MAC routing table using the [mac-table-size](#) statement at the **[edit routing-instances *routing-instance-name* protocols evpn]** hierarchy level.

You can optionally configure the [packet-action drop](#) option to specify that packets for new source MAC addresses be dropped once the MAC address limit is reached. If you do not configure this option, packets for new source MAC addresses are forwarded.

12. Disable MAC learning by including the [no-mac-learning](#) statement at either the **[edit routing-instances *routing-instance-name* protocols evpn]** hierarchy level to apply this behavior to all of the devices configured for an EVPN routing instance or at the **[edit routing-instances *routing-instance-name* protocols evpn interface *interface-name*]** hierarchy level to apply this behavior to just one of the CE devices.

Related Documentation

- [Configuring Policies for the VRF Table on PE Routers in VPNs on page 25](#)
- [Configuring Routing Instances on PE Routers in VPNs on page 9](#)
- [Tracing EVPN Traffic and Operations on page 242](#)

Tracing EVPN Traffic and Operations

To configure the EVPN routing instance to trace a variety of different parameters related to EVPN operation:

1. Specify the name of one or more EVPN trace files using the **file** option for the **traceoptions** statement at the **[edit routing-instances routing-instance-name protocols evpn]** 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 **flag** option allows you to specify the scope of the trace by including one of the following sub-options:

- **all**—All EVPN tracing options
- **error**—Error conditions
- **general**—General events
- **mac-database**—MAC route database in the EVPN routing instance
- **nlri**—EVPN advertisements received or sent by means of the BGP
- **normal**—Normal events
- **oam**—OAM messages
- **policy**—Policy processing
- **route**—Routing information

- **state**—State transitions
- **task**—Routing protocol task processing
- **timer**—Routing protocol timer processing
- **topology**—EVPN topology changes caused by reconfiguration or advertisements received from other PE routers using BGP

You can also specify one of the following modifiers for any of the traceoptions flags:

- **detail**—Provide detailed trace information.
- **disable**—Disable this trace flag.
- **receive**—Trace received packets.
- **send**—Trace sent packets.

- Related Documentation**
- [Configuring EVPN Routing Instances on page 239](#)
 - [traceoptions on page 1210](#)

CHAPTER 19

Configuring EVPN Multihoming

- [EVPN Multihoming Overview on page 245](#)
- [Configuring EVPN Active-Standby Multihoming on page 261](#)
- [Example: Configuring EVPN Active-Standby Multihoming on page 264](#)

EVPN Multihoming Overview

- [Introduction to EVPN Multihoming on page 245](#)
- [Understanding EVPN Multihoming Concepts on page 247](#)
- [EVPN Multihoming Mode of Operation on page 249](#)
- [EVPN Multihoming Implementation on page 249](#)
- [Designated Forwarder Election on page 258](#)

Introduction to EVPN Multihoming

An Ethernet VPN (EVPN) is comprised of customer edge (CE) devices that are connected to provider edge (PE) devices, which form the edge of the MPLS infrastructure. A CE device can be a host, a router, or a switch. The PE devices provide Layer 2 virtual bridge connectivity between the CE devices. There can be multiple EVPNs in the provider network. Learning between the PE routers occurs in the control plane using BGP, unlike traditional bridging, where learning occurs in the data plane.



NOTE: Prior to Junos OS Release 15.1, EVPN functionality support on MX Series routers was limited to routers using MPC and MIC interfaces only. However, starting with Junos OS Release 15.1, MX Series routers using DPCs can be leveraged to provide EVPN support on the CE device-facing interface.

DPC support for EVPN is provided with the following considerations:

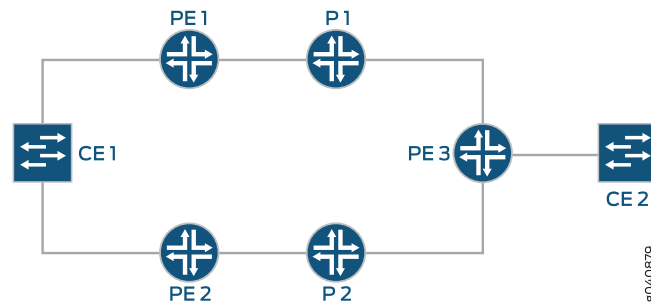
- DPCs provide support for EVPN in the active-standby mode of operation including support for the following:
 - EVPN instance (EVI)
 - Virtual switch (VS)
 - Integrated routing and bridging (IRB) interfaces
- DPCs intended for providing the EVPN active-standby support should be the CE device-facing line card. The PE device interfaces in the EVPN domain should use only MPC and MIC interfaces.

The EVPN multihoming feature enables you to connect a customer site to two or more PE devices to provide redundant connectivity. A CE device can be multihomed to different PE devices or the same PE device. A redundant PE device can provide network service to the customer site as soon as a failure is detected. Thus, EVPN multihoming helps to maintain EVPN service and traffic forwarding to and from the multihomed site in the event of the following types of network failures:

- PE device to CE device link failure
- PE device failure
- MPLS-reachability failure between the local PE device and a remote PE device

[Figure 20 on page 247](#) illustrates how a CE device could be multihomed to two PE routers. Device CE1 is multihomed to Routers PE1 and PE2. Device CE2 has two potential paths to reach Device CE1, and depending on the multihoming mode of redundancy, only one path or all paths are active at any one time. The multihoming mode of operation also determines which PE router or routers forward traffic to the CE device. The PE router forwarding traffic to the CE device (also called a designated forwarder) uses MPLS LSP or GRE tunnels to forward traffic. If a failure occurs over this path, a new designated forwarder is elected to forward the traffic to Device CE1.

Figure 20: CE Device Multihomed to Two PE Routers



Understanding EVPN Multihoming Concepts

Figure 21 on page 248 explains the EVPN multihoming concepts using a simple EVPN network topology.

- **Ethernet segment**—When a CE device is multihomed to two or more PE routers, the set of Ethernet links constitutes an Ethernet segment. An Ethernet segment appears as a link aggregation group (LAG) to the CE device.

The links from Routers PE1 and PE2 to Device CE1 form an Ethernet segment.

In active-standby multihoming, the links that constitute an Ethernet segment form a bridge domain. In active-active multihoming, an Ethernet segment appears as a LAG to the CE device.

- **ESI**—An Ethernet segment must have a unique nonzero identifier, called the Ethernet segment identifier (ESI). The ESI is encoded as a 10 octet integer. When manually configuring an ESI value, the most significant octet, known as the type byte, must be 00. When a single-homed CE device is attached to an Ethernet segment, the entire ESI value is zero.

The Ethernet segment of the multihomed Device CE1 has an ESI value of **00:11:22:33:44:55:66:77:88:99** assigned. The single-homed Device CE2 has an ESI value of 0.

- **EVI**—An EVPN instance (EVI) is an EVPN routing and forwarding instance spanning across all the PE routers participating in that VPN. An EVI is configured on the PE routers on a per-customer basis. Each EVI has a unique route distinguisher and one or more route targets.

An EVI is configured on Routers PE1, PE2, and PE3.

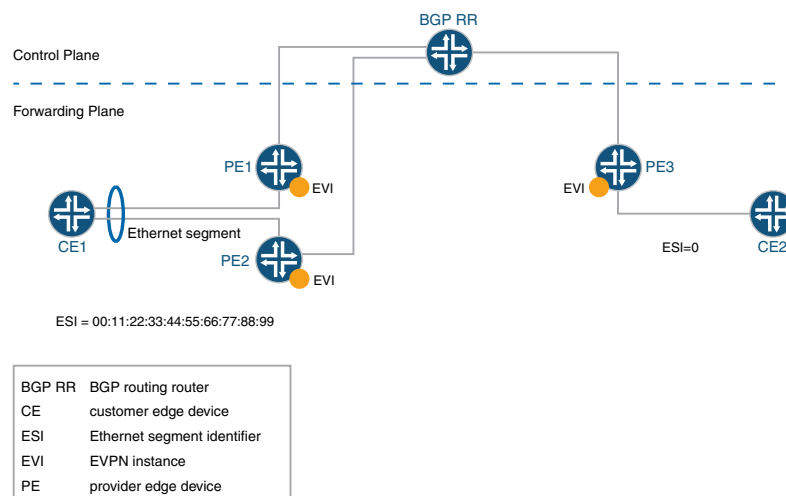
- **Ethernet tag**—An Ethernet tag identifies a particular broadcast domain, such as a VLAN. An EVPN instance consists of one or more broadcast domains. Ethernet tags are assigned to the broadcast domains of a given EVPN instance by the provider of that EVPN. Each PE router in that EVPN instance performs a mapping between broadcast domain identifiers understood by each of its attached CE devices and the corresponding Ethernet tag.

- **Ethernet segment route**—The PE routers that are connected to a multihomed CE device use BGP Ethernet segment route messages to discover that each of the PE routers is connected to the same Ethernet segment. The PE routers advertise the Ethernet segment route, which consists of an ESI and ES-import extended community.

Routers PE1 and PE2 advertise an ES route with an ES-import extended community (along with other extended communities like the route target). The PE routers also construct a filter based on an ES-import extended community, which results in only these PE routers importing the ES route and identifying that they are connected to the same Ethernet segment.

- **Extended community**—An extended community is similar in most ways to a regular community. EVPNs use extended communities because the 4-octet regular community value does not provide enough expansion and flexibility. An extended community is an eight-octet value divided into two main sections.
- **BUM traffic**—This type of traffic is sent to multiple destinations, including broadcast traffic, unknown unicast traffic that is broadcast in the Ethernet segment, and multicast traffic.
- **DF**—When a CE device is multihomed to two or more PE routers, either one or all of the multihomed PE routers are used to reach the customer site depending on the multihoming mode of operation. The PE router that assumes the primary role for forwarding BUM traffic to the CE device is called the designated forwarder (DF).
- **BDF**—Each router in the set of other PE routers advertising the autodiscovery route per Ethernet segment for the same ESI, and serving as the backup path in case the DF encounters a failure, is called a backup designated forwarder (BDF). A BDF is also called a non-DF router.
- **DF election**—On every Ethernet segment, the PE routers participate in a procedure called designated forwarder (DF) election to select the DF and the BDF PE routers.

Figure 21: Simple EVPN Topology



EVPN Multihoming Mode of Operation

The different modes of operation for EVPN multihoming include:

- **Single**—When a PE router is connected to a single-homed customer site, this mode is in operation. This is the default mode of operation, and does not require Ethernet segment values to be configured.
- **Active-Standby**—When only a single PE router, among a group of PE routers attached to an Ethernet segment, is allowed to forward traffic to and from that Ethernet segment, the Ethernet segment is defined to be operating in the active-standby redundancy mode.

To configure the active-standby mode, include the ESI value and the **single-active** statement under the **[edit interfaces]** hierarchy level.

- **Active-Active**—When all PE routers attached to an Ethernet segment are allowed to forward traffic to and from the Ethernet segment, the Ethernet segment is defined to be operating in an active-active redundancy mode.



NOTE: Starting with Junos OS Release 14.1X53-D30, QFX5100 switches support the active-active mode of operation for EVPN multihoming. In this scenario, QFX5100 switches function as top-of-rack (ToR) switches in the data center for virtual networks. EVPN multihoming active-active functionality is used to provide access to the bare-metal servers connected to the ToR switches.

EVPN Multihoming Implementation

The EVPN active-standby multihoming mode of operation provides redundancy for access link failures and PE node failure for the multihomed CE device, and is based on the EVPN *draft-ietf-l2vpn-evpn-03*.

The Junos OS implementation of the EVPN multihoming active-standby mode of operation includes the following:

- [New BGP NLRI on page 250](#)
- [New Extended Communities on page 252](#)
- [New EVPN Route Types on page 253](#)
- [Update to the MAC Forwarding Table on page 254](#)
- [Traffic Flow on page 255](#)
- [Aliasing on page 256](#)
- [Sample Configuration on page 257](#)

New BGP NLRI

To support EVPN multihoming, the following new BGP network layer reachability information (NLRI) routes have been introduced:

- [Autodiscovery Route per Ethernet Segment on page 250](#)
- [Ethernet Segment Route on page 251](#)

Autodiscovery Route per Ethernet Segment

- [Autodiscovery Route Features on page 250](#)
- [Autodiscovery Route Advertisement on page 250](#)
- [Autodiscovery Route Withdrawal on page 250](#)

Autodiscovery Route Features

The autodiscovery route NLRI features include:

- This is a Type 1 mandatory route, used for fast convergence and for advertising the split horizon label. It is also known as the mass withdraw route.
- Type 1 route distinguishers are used with the IP address (loopback) of the originating PE router as the route distinguisher value.
- This route carries the ESI in the NLRI (nonzero when it is a multihomed PE, zero otherwise).
- The split horizon label is per ESI only, and carries an explicit NULL (0).
- The bit in the active-standby flag field in the ESI label extended community is used for signaling the active-standby mode (bit set).
- The 3-byte label values in the NLRI and the Ethernet tag is zero.
- This route is advertised and imported by all multihomed and remote PE routers that share the same EVI on the advertising ESI.

Autodiscovery Route Advertisement

- Active-standby mode

In active-standby mode, the designated forwarder (DF) advertises the autodiscovery route per Ethernet segment with an ESI MPLS label extended community that has the standby bit set to 1. The autodiscovery route is advertised per ESI, and the ESI label is set to 0 when active-standby mode is in operation.

The autodiscovery route is imported by all the multihomed and remote PE routers that are part of the EVI. On receiving the autodiscovery route, the PE routers in the network topology learn that active-standby multihoming mode is in operation for the ESI advertised.

Autodiscovery Route Withdrawal

The autodiscovery route per Ethernet segment withdrawal is also referred to as the mass withdrawal. The mass withdrawal feature is used when there is a link failure on the ESI, or when the ESI configuration changes.

When the link between a multihomed CE device and a multihomed PE device fails, the PE device withdraws the autodiscovery route per Ethernet segment. In such a case, the mass withdrawal feature is handled in the following ways by the other PE devices:

- Remote PE device

When a remote PE device receives the BGP update for mass withdrawal, the following is performed at the remote PE device:

1. The current next hop to reach the remote ESI or CE device is deleted.
2. A new next hop through the remaining multihomed PE devices is created to reach the remote ESI or CE device.
3. All the MAC routes behind the CE device are updated with the newly created next hop.

- Other multihomed PE device

As a result of the mass withdrawal, load balancing on the multihomed CE device happens because of the following:

- When the other multihomed PE devices receive the same set of MAC addresses on the link to the concerned ESI.

In this case, the local routes are preferred. If the remote routes learned from the DF PE device gets withdrawn, it does not affect routes pointing to the local ESI.

- When the other multihomed PE devices have not received the same set of MAC addresses on the link to the concerned ESI.

In this case, the PE devices install the MAC routes pointing to the concerned ESI, although the MACs are remotely learned from the DF PE device. When the DF PE device withdraws these routes, the withdrawn routes are flushed. Packets that are destined to the flushed MAC addresses are flooded on all the local segments.

Ethernet Segment Route

- [Ethernet Segment Route Features on page 251](#)
- [Ethernet Segment Route Advertisement on page 252](#)

Ethernet Segment Route Features

The Ethernet segment route NRLI features include:

- This is a Type 4 route. The purpose of this route is to enable the PE routers connected to the same Ethernet segment to automatically discover each other with minimal configuration on exchanging this route.
- This route is associated with an ES-import extended community with an ESI value condensed to 6 bytes, similar to a route target.
- This route is advertised and imported only by PE routers that are multihomed on the advertising Ethernet segment.

Ethernet Segment Route Advertisement

The Ethernet segment route is exchanged among all the PE routers within a data center with the ES-import extended community. The ES-import extended community is constructed based on the ESI PE routers that are multihomed, and the Ethernet segment route carries the ESI value related to the Ethernet segment on which the PE routers are multihomed.

The Ethernet segment routes are filtered based on the ES-import extended community, such that only the PE routers that are multihomed on the same Ethernet segment import this route. Each PE router that is connected to a particular Ethernet segment constructs an import filtering rule to import a route that carries the ES-import extended community.

New Extended Communities

An extended community is similar in most ways to a regular community. Some networking implementations, such as virtual private networks (VPNs), use extended communities because the 4-octet regular community value does not provide enough expansion and flexibility. An extended community is an 8-octet value divided into two main sections.

To support active-standby multihoming, the following extended communities have been introduced:

- [ESI-Import on page 252](#)
- [Split Horizon on page 252](#)

ESI-Import

This extended community is attached to the ES route, and is populated from the ESI-import value extracted from the configured ESI value under the interface. To solve the problem of a conflict with another regular route target, the type is set to 0x06, which has been allocated by IANA.

The ESI-import extended community route target populates the list of import route targets configured for the special instance from where the ES route using this community is advertised.

Therefore, incoming ESI routes with the same ESI-import value in the extended community are imported by the PE routers, if the PE router is configured with an Ethernet segment that has the same ESI value. Once the PE router receives a set of these ESI routes that have the same ESI-import extended community value, the DF and BDF election can be done locally.



NOTE: When the ESI-import extended community is not created implicitly, a policy should be configured to attach all the route targets to the autodiscovery route per Ethernet segment.

Split Horizon

- Split horizon signaling

The split horizon extended community is attached to the autodiscovery route per Ethernet segment. The value of the extended community is the split horizon or the Poisson label itself, which is 3 bytes, and is advertised as an opaque attribute.

- Split horizon advertisement
 - In active-standby mode, the standby bit in the split horizon extended community is set to 1, and the ESI split horizon label is set to 0.
- Split horizon MPLS routes

The DF PE device advertises an autodiscovery route per Ethernet segment with a split horizon label A, and an inclusive multicast route with label B for BUM traffic forwarding. On the DF, the BUM packet from the core can come with following labels:

- When the non-DF PE devices receive a BUM packet on their single-homed ESIs, the BUM packet is sent to the DF PE device with multicast label B.
- When the non-DF PE devices receive a BUM packet on ESI1, the BUM packet is sent to the DF PE device with two MPLS labels — the multicast label B as the outer label, and the split horizon label A as the inner label.

In the EVPN multihoming scenario, the multicast label B has the S-bit set to 1 when it is the only label in the label stack. In this case, the BUM packet needs to be flooded on all the local ESIs on the DF PE device. But the label B has the S-bit set to 0 when split horizon label A is the innermost label in the label stack. In this case, the BUM packets need to be flooded on all local ESIs on the DF PE device, except the ESI that maps to the split horizon label A.

Assuming that packets originated from a multihomed CE device to a non-DF PE device on multihomed segment ESI1, when the non-DF PE device sends this packet to the DF PE device, the ESI label that the DF advertised to the non-DF PE device in its autodiscovery route per Ethernet segment is pushed first. The non-DF PE device also pushes the inclusive multicast label that the DF PE device advertised in its inclusive multicast route and further pushes the LSP label. The MPLS header thus contains two labels within a 32-bit field.

The base EVPN functionality uses a table-next hop to stitch the MPLS table with its corresponding EVPN EVI table. In the EVPN EVI table, the mac-lookup is performed to switch the packet.

The following routes are programmed in the mpls.0 table for EVPN multicast:

- The (multicast-label, S=1) route points to the EVPN-EVI table-next hop.
- The (multicast-label, S=0) route points to the MPLS table-next hop. This route loops the packet back to the MPLS table after popping the multicast-label.
- The (split horizon-label) route points to the EVPN-EVI table-next hop. This is the same table-next hop that is used by the multicast-label, S=1 route.

New EVPN Route Types

EVPN multihoming mode supports the following EVPN route types:

- Autodiscovery route per Ethernet segment
- Autodiscovery route per EVPN instance (EVI)
- Ethernet segment route

These route types conform to the following naming convention:

<route-type>:<RD>::<esi>::<route-specific>/304

For example:

Autodiscovery route per Ethernet segment—1:10.255.0.2:0::112233445566778899::0/304

Autodiscovery route per EVI—1:100.100.100.1:1::22222222222222222222::0/304

Ethernet segment route—4:10.255.0.1:0::112233445566778899:10.255.0.1/304

where:

- **route-type**—Type of EVPN route.
 - 1—Autodiscovery route per Ethernet segment.
 - 1—Autodiscovery route per EVI.
 - 4—Ethernet segment route.

- **RD**—Route distinguisher value.

The route distinguisher value is set to the IP address of the PE router followed by 0.

- **esi**—Ethernet segment identifier. Displayed as 10 bytes of hexadecimal bytes, and leading 00 bytes are not displayed.
- **route-specific**—Differs per route type.
 - Autodiscovery route per Ethernet segment and autodiscovery route per EVI—This value is an MPLS label.



NOTE: The MPLS label is displayed in the extensive output, although it is not included in the prefix.

- Ethernet segment route—This value is the originating IP address.
- **304**—Maximum number of bits in an EVPN route. This is not very useful information and could be removed from the display. However, it might be useful in quickly identifying an EVPN route, either visually or with match operators.

Update to the MAC Forwarding Table

In active-standby EVPN multihoming, the MAC addresses are treated as routable addresses, and the MP-IBGP protocol is used to carry the customer MAC addresses. MAC learning at the PE routers does not occur in the data plane but in the control plane. This leads to more control applied in terms of the learning mechanism.

A PE router performs MAC learning in the data plane for packets coming from a customer network for a particular EVI. For CE MAC addresses that are behind other PE routers, the MAC addresses are advertised in BGP NLRI using a new MAC advertisement route type.

The MAC learning is of two types:

- Local MAC learning—PE routers must support the local MAC learning process through standard protocols.
- Remote MAC learning—Once the local learning process is completed, the PE routers can advertise the locally learned MAC address to remote PE router nodes through MP-IBGP. This process of receiving the remote MAC addresses of attached customers through MP-IBGP is known as the remote MAC learning process.

The MAC advertisement route type is used to advertise locally learned MAC addresses in BGP to remote PE routers. If an individual MAC address is advertised, the IP address field corresponds to that MAC address. If the PE router sees an ARP request for an IP address from a CE device, and if the PE router has the MAC address binding for that IP address, the PE router performs ARP proxy and responds to the ARP request.



NOTE: The ARP proxy is performed only for the gateway and not for the host.

The MPLS label field depends on the type of allocation. The PE router can advertise a single MPLS label for all MAC addresses per EVI, which requires the least number of MPLS labels and saves the PE router memory. However, when forwarding to the customer network, the PE router must perform a MAC lookup which can cause a delay and increase the number of CPU cycles.

Traffic Flow

In EVPN multihoming, traffic flow is performed in the forwarding-plane. Flood routes are created for flooding the packets, and are used in the following scenarios:

- When a packet is received on a local ESI
- When a packet is received from the core

The traffic flows in EVPN multihoming can be based on the two traffic types:

- Unicast traffic

Unicast traffic is a point-to-point communication with one sender and one receiver. In a multihomed EVPN, unicast traffic is forwarded as follows:

- In active-standby mode
 - CE to core—Traffic is learned and forwarded by the DF PE router.
 - Core to CE—The remote PE router learns the MAC addresses from the DF, and forwards all unicast traffic to the DF PE router.
- BUM traffic

Traffic that is sent to multiple destinations, including broadcast traffic, unknown unicast traffic that is broadcast in the Ethernet segment, and multicast traffic is known as BUM traffic. In a multihomed EVPN, BUM traffic is forwarded as follows:

- In active-standby mode
 - CE to core—The CE device floods any BUM traffic to all the links in the Ethernet segment. The DF PE router with the active path forwards the BUM packets to the core. The BDF PE router in the standby mode drops all the traffic from the CE device, because the EVPN multihomed status of the interface is in blocking state.
 - Core to CE—The remote PE routers flood all BUM traffic to both the DF and BDF PE routers. Only the DF forwards the BUM traffic to the CE device. The BDF PE router drops all the traffic, because the EVPN multihomed status of the interface is in blocking state.

Aliasing

Aliasing is the ability of a remote PE device to load balance Layer 2 unicast traffic on all the other PE devices that have same Ethernet segment towards a CE device.

- [Aliasing and Autodiscovery Routes on page 256](#)
- [Aliasing and Label Route on page 256](#)
- [Aliasing and Unicast Packet Forwarding on page 257](#)

Aliasing and Autodiscovery Routes

Autodiscovery routes from Routers PE2 and PE3 can come in any order. As a result, these routes are installed by the Layer 2 process as follows:

1. After receiving MAC1 from Router PE1, and if any autodiscovery routes have not been received by Router PE4, MAC1 is programmed by PE4 with a next hop pointing toward Router PE1. When PE4 receives the autodiscovery route from Router PE2 for the same ESI, the next hop is installed so the traffic for MAC1 is load-balanced to Routers PE1 and PE2. When PE4 receives the autodiscovery route from Router PE3 for the same ESI, the next hop is updated to load-balance the traffic for MAC1 among Routers PE1, PE2, and PE3.
2. If Router PE4 has already received the autodiscovery routes from more than one PE device (PE1, PE2, and PE3), PE4 installs the MAC routes with the multi-destination next hop.

Aliasing and Label Route

Any PE device that advertises the autodiscovery route per EVI with a valid MPLS label programs the advertised label in the mpls.0 routing table. For instance, if Router PE2 advertised the autodiscovery route per EVI with label A, the mpls.0 entry is as follows:

Label A route points to the EVPN-EVI table-next hop.

When the remote Router PE4 sends a unicast data packet toward Router PE2 with this label A, lookup is done in Router PE2's forwarding table, and as a result of this lookup, the packet is forwarded on ESI1.

Aliasing and Unicast Packet Forwarding

When the unicast packets for MAC1 come from the remote Router PE4 to Router PE2, there could be two cases:

- Router PE2 also received the same set of MACs on its link to ES11—In this case, local routes are preferred and as a result of the MAC lookup, packets are forwarded to ES11.
- Router PE2 has not received the same set of MACs on its link to ES11—In this case, Router PE2 still installs MAC routes pointing to ES11, although MACs are remotely learned from Router PE1. As a result, the packets are forwarded to ES11.

Sample Configuration

The following is a sample configuration for EVPN active-standby multihoming on the following types of interfaces:

- Ethernet interface configuration

```
ge-0/1/2 {
  encapsulation ethernet-bridge;
  esi XX:XX:XX:XX:XX:XX:XX:XX:XX:XX;
  unit 0 {
    family bridge;
  }
}
```

- Single VLAN interface configuration

```
ge-0/1/3 {
  encapsulation extended-vlan-bridge;
  esi XX:XX:XX:XX:XX:XX:XX:XX:XX:XX;
  vlan-tagging
  unit 0 {
    family bridge;
    vlan-id 1;
  }
}
```



NOTE:

- An ESI value of 0 and all FFs are reserved and are not used for configuring a multihomed Ethernet segment.
- Two interfaces in the same EVI cannot be configured with the same ESI value.

The following is a sample routing instance configuration for EVPN active-standby multihoming:

- Routing instance configuration

```
routing-instances {
  evpn-0 {
    instance-type evpn;
  }
}
```

```

route-distinguisher value;
vrf-target value;
vlan-id vlan-ID;
interface ge-0/1/2.0;
interface ge-1/1/1.0;
interface ge-2/2/2.0;
protocols {
  evpn {
    designated-forwarder-election hold-time time;
  }
}
}
}

```



NOTE: With the active-standby mode configuration, the autodiscovery route per Ethernet segment is advertised with the active-standby bit set to 1 for this Ethernet segment.

Designated Forwarder Election

The following sections discuss DF election:

- [DF Election Roles on page 258](#)
- [DF Election Procedure on page 259](#)
- [DF Election Trigger on page 259](#)
- [DF Election for Virtual Switch on page 260](#)
- [Handling Failover on page 260](#)

DF Election Roles

The designated forwarder (DF) election process involves selecting the following two roles:

- **DF**—The MAC address from the customer site is reachable only through the PE router announcing the associated MAC advertisement route. This PE router is the primary PE router that is selected to forward BUM traffic to the multihomed CE device, and is called the designated forwarder (DF) PE router.
- **BDF**—Each PE router in the set of other PE routers advertising the autodiscovery route per Ethernet segment for the same ESI, and serving as the backup path in case the DF encounters a failure, is called a backup designated forwarder (BDF) or a non-DF (non-designated forwarder).

As a result of the DF election process, if a local PE router is elected as the BDF, the multihomed interface connecting to the customer site is put into a blocking state for the active-standby mode. The interface remains in the blocking state until the PE router is elected as the DF for the Ethernet segment that the interface belongs to.

DF Election Procedure

The default procedure for DF election at the granularity of the ESI and EVI is referred to as service carving. With service carving, it is possible to elect multiple DFs per Ethernet segment (one per EVI) in order to perform load-balancing of multidestination traffic destined to a given Ethernet segment. The load-balancing procedures carve up the EVI space among the PE nodes evenly, in such a way that every PE is the DF for a disjoint set of EVIs.

The procedure for service carving is as follows:

1. When a PE router discovers the ESI of the attached Ethernet segment, it advertises an autodiscovery route per Ethernet segment with the associated ES-import extended community attribute.
2. The PE router then starts a timer (default value of 3 seconds) to allow the reception of the autodiscovery routes from other PE nodes connected to the same Ethernet segment. This timer value must be the same across all the PE routers connected to the same Ethernet segment.

The default wait timer can be overwritten using the **designated-forwarder-election hold-time** configuration statement.

3. When the timer expires, each PE router builds an ordered list of the IP addresses of all the PE nodes connected to the Ethernet segment (including itself), in increasing numeric order. Every PE router is then given an ordinal indicating its position in the ordered list, starting with 0 as the ordinal for the PE with the numerically lowest IP address. The ordinals are used to determine which PE node is the DF for a given EVI on the Ethernet segment.
4. The PE router that is elected as the DF for a given EVI unblocks traffic for the Ethernet tags associated with that EVI. The DF PE unblocks multidestination traffic in the egress direction toward the Ethernet segment. All the non-DF PE routers continue to drop multidestination traffic (for the associated EVIs) in the egress direction toward the Ethernet segment.

DF Election Trigger

In general, a DF election process is triggered in the following conditions:

- When an interface is newly configured with a nonzero ESI, or when the PE router transitions from an isolated-from-the-core (no BGP session) state to a connected-to-the-core (has established BGP session) state, a wait timer is imposed. By default, the interface is put into a blocking state until the PE router is elected as the DF.
- After completing a DF election process, a PE router receives a new Ethernet segment route or detects the withdrawal of an existing Ethernet segment route, without an imposed wait timer.
- When an interface of a non-DF PE router recovers from a link failure, the PE router has no knowledge of the wait time imposed by other PE routers. As a result, no wait timer is imposed for the recovered PE router to avoid traffic loss.

DF Election for Virtual Switch

The virtual switch allows multiple bridge domains in a single EVPN instance (EVI). The virtual switch also supports trunk and access ports. Junos OS allows flexible Ethernet services on the port, therefore different VLANs on a single port can be part of different EVIs.

The DF election for virtual switch depends on the following:

- Port mode—Sub-interface, trunk interface, and access port
- EVI mode—Virtual switch with EVPN, EVPN-EVI

In the virtual switch, multiple Ethernet tags can be associated with a single EVI, wherein the numerically lowest Ethernet tag value in the EVI is used for the DF election.

Handling Failover

A failover can happen due to two things:

- When the DF PE router loses its DF role.
- When there is a link or port failure on the DF PE router.

On losing the DF role, the customer-facing interface on the DF PE router is put in the blocking state.

In the case of link or port failure, a DF election process is triggered, resulting in the BDF PE router to be selected as the DF. At that time, flow of traffic is affected as follows:

- [Unicast Traffic on page 260](#)
- [BUM Traffic on page 260](#)

Unicast Traffic

- CE to Core—The CE device continues to flood traffic on all the links. The previous BDF PE router changes the EVPN multihomed status of the interface from the blocking state to the forwarding state, and traffic is learned and forwarded through this PE router.
- Core to CE—The failed DF PE router withdraws the autodiscovery route per Ethernet segment and the locally-learned MAC routes, causing the remote PE routers to redirect traffic to the BDF.



NOTE: The transition of the BDF PE router to the DF role can take some time, causing the EVPN multihomed status of the interface to continue to be in the blocking state, resulting in traffic loss.

BUM Traffic

- CE to Core—All the traffic is routed toward the BDF.
- Core to CE—The remote PE routers flood the BUM traffic in the core.

Release History Table

Release	Description
14.X53-D30	Starting with Junos OS Release 14.1X53-D30, QFX5100 switches support the active-active mode of operation for EVPN multihoming.

Related Documentation

- [Example: Configuring EVPN Active-Standby Multihoming on page 264](#)

Configuring EVPN Active-Standby Multihoming

You can configure an Ethernet VPN (EVPN) with multihoming support to provide multihoming functionality with active-standby redundancy mode of operation in the EVPN and virtual switch routing instance. This mode enables autodiscovery of Ethernet segments, Ethernet segment route construction, and Ethernet segment identifier (ESI) label assignment.

When configuring active-standby EVPN multihoming, be aware of the following limitations:

- An interface or ESI can be attached to more than one EVPN instance (EVI), with a maximum limit of 200 EVIs per ESI.
- For an EVPN routing instance, only one logical interface per physical interface or ESI can be attached to an EVI.
- For a virtual switch routing instance, only one logical interface per physical interface or ESI can be configured under a bridge domain.
- All the PE routers in the network topology should be running Junos OS Release 14.1 or later releases, which are based on the EVPN draft-ietf-l2vpn-evpn-03. Junos OS releases prior to 14.1 support the older version of the EVPN draft, causing interoperability issues when Junos OS Release 14.1 and a previous release are running.

Before you begin:

1. Configure the router interfaces.
2. Configure the router ID and autonomous system number for the device.
3. Configure OSPF or any other IGP protocol.
4. Configure a BGP internal group.
5. Include the EVPN signaling network layer reachability information (NLRI) to the internal BGP group.
6. Configure LDP.
7. Configure MPLS.
8. Configure RSVP MPLS LSP or GRE tunnels.

To configure the PE device:

1. Enable EVPN active-standby multihoming on the multihomed interfaces.

```
[edit interfaces]
user@PE1# set interface-name vlan-tagging
user@PE1# set interface-name encapsulation flexible-ethernet-services
user@PE1# set interface-name esi esi-value
user@PE1# set interface-name esi single-active
user@PE1# set interface-name unit 0 encapsulation vlan-bridge
user@PE1# set interface-name unit 0 vlan-id VLAN-ID
```

For example:

```
[edit interfaces]
user@PE1# set ge-0/0/4 vlan-tagging
user@PE1# set ge-0/0/4 encapsulation flexible-ethernet-services
user@PE1# set ge-0/0/4 esi 00:22:44:66:88:00:22:44:66:88
user@PE1# set ge-0/0/4 esi single-active
user@PE1# set ge-0/0/4 unit 0 encapsulation vlan-bridge
user@PE1# set ge-0/0/4 unit 0 vlan-id 300
```

2. In configuration mode, go to the following hierarchy level:

```
[edit]
user@PE1# edit routing-instances
```

3. Configure the virtual switch routing instance.

```
[edit routing-instances]
user@PE1# set virtual-switch-instance instance-type virtual-switch
```

4. Configure the extended VLAN list for the virtual switch routing instance.

```
[edit routing-instances]
user@PE1# set virtual-switch-instance protocols evpn extended-vlan-list VLAN-ID
```

5. Set the type for the bridging domain in the virtual switch routing instance.

```
[edit routing-instances]
user@PE1# set virtual-switch-instance bridge-domains bridge-domain-name
domain-type bridge
```

6. Set the VLAN identifier for the bridging domain in the virtual switch routing instance.

```
[edit routing-instances]
user@PE1# set virtual-switch-instance bridge-domains bridge-domain-name vlan-id
VLAN-ID
```

7. Configure the interfaces for the virtual switch routing instance.

```
[edit routing-instances]
user@PE1# set virtual-switch-instance bridge-domains bridge-domain-name interface
interface-name
user@PE1# set virtual-switch-instance bridge-domains bridge-domain-name
routing-interface interface-name
```

8. Configure the route distinguisher for the virtual switch routing instance.

```
[edit routing-instances]
user@PE1# set virtual-switch-instance route-distinguisher route-distinguisher-value
```

9. Configure the VPN routing and forwarding (VRF) target community for the virtual switch routing instance.

```
[edit routing-instances]
```

```
user@PE1# set virtual-switch-instance vrf-target vrf-target
```

10. Configure the EVPN routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance instance-type evpn
```

11. Set the VLAN identifier for the bridging domain in the EVPN routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance vlan-id VLAN-ID
```

12. Configure the interface names for the EVPN routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance interface interface-name
user@PE1# set evpn-instance routing-interface interface-name
```

13. Configure the route distinguisher for the EVPN routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance route-distinguisher route-distinguisher-value
```

14. Configure the VPN routing and forwarding (VRF) target community for the EVPN routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance vrf-target vrf-target
```

15. Configure the VRF routing instance.

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

16. Configure the interface names for the VRF routing instance.

```
[edit routing-instances]
user@PE1# set vrf-instance interface interface-name
```

17. Configure the route distinguisher for the VRF routing instance.

```
[edit routing-instances]
user@PE1# set vrf-instance route-distinguisher route-distinguisher-value
```

18. Configure the VPN routing and forwarding (VRF) target community for the VRF routing instance.

```
[edit routing-instances]
user@PE1# set vrf-instance vrf-target vrf-target
user@PE1# set vrf-instance vrf-table-label
```

19. Verify and commit the configuration.

For example:

```
[edit routing-instances]
user@PE1# set ALPHA instance-type virtual-switch
user@PE1# set ALPHA route-distinguisher 10.255.0.1:100
user@PE1# set ALPHA vrf-target target:100:100
user@PE1# set ALPHA protocols evpn extended-vlan-list 100
user@PE1# set ALPHA bridge-domains ONE domain-type bridge
user@PE1# set ALPHA bridge-domains ONE vlan-id 100
user@PE1# set ALPHA bridge-domains ONE interface ae0.0
```

```
user@PE1# set ALPHA bridge-domains ONE interface ge-0/0/2.0
user@PE1# set ALPHA bridge-domains ONE routing-interface irb.0
user@PE1# set BETA instance-type evpn
user@PE1# set BETA vlan-id 300
user@PE1# set BETA interface ge-0/0/4.0
user@PE1# set BETA interface ae1.0
user@PE1# set BETA routing-interface irb.1
user@PE1# set BETA route-distinguisher 10.255.0.1:300
user@PE1# set BETA vrf-target target:300:300
user@PE1# set DELTA instance-type vrf
user@PE1# set DELTA interface irb.0
user@PE1# set DELTA interface irb.1
user@PE1# set DELTA route-distinguisher 10.255.0.1:200
user@PE1# set DELTA vrf-target target:200:200
user@PE1# set DELTA vrf-table-label

[edit]
user@PE1# commit
commit complete
```

Related Documentation

- [Example: Configuring EVPN Active-Standby Multihoming on page 264](#)

Example: Configuring EVPN Active-Standby Multihoming

This example shows how to configure Ethernet VPN (EVPN) for multihomed customer edge (CE) devices in an EVPN, virtual switch, and VRF routing instance, and with an integrated routing and bridging (IRB) interface configuration.

- [Requirements on page 264](#)
- [Overview and Topology on page 265](#)
- [Configuration on page 267](#)
- [Verification on page 278](#)

Requirements

This example uses the following hardware and software components:

- Four MX Series 3D Universal Edge Routers with MPC interfaces only, where:
 - Two devices are configured as provider edge (PE) routers connected to a common multihomed customer site.
 - One device is configured as a remote PE router connected to a single-homed customer site.
- Eight customer edge (CE) devices, where:
 - Two CE devices are multihomed.
 - Two CE devices are single-homed for each of the PE routers.
- Junos OS Release 14.1 or later running on all the PE routers.



NOTE: Junos OS Release 14.1 and later releases are based on the EVPN draft-ietf-l2vpn-evpn-03. Releases prior to 14.1, support the older version of the EVPN draft, causing interoperability issues when Junos OS Release 14.1 and a previous release are running.

Before you begin:

1. Configure the router interfaces.
2. Configure OSPF or any other IGP protocol.
3. Configure BGP.
4. Configure LDP.
5. Configure MPLS.
6. Configure RSVP MPLS LSP or GRE tunnels.

Overview and Topology

Starting with Junos OS Release 14.1, the EVPN solution on MX Series routers with MPC interfaces is extended to provide multihoming functionality with active-standby mode of operation. The multihoming functions include autodiscovery of Ethernet segments, Ethernet segment route construction, and Ethernet segment identifier (ESI) label assignment.



NOTE: Prior to Junos OS Release 15.1, the EVPN functionality support on MX Series Routers was limited to routers using MPC and MIC interfaces only. However, starting with Junos OS Release 15.1, MX Series Routers using DPCs can be leveraged to provide EVPN support on the CE device-facing interface.

The DPC support for EVPN is provided with the following considerations:

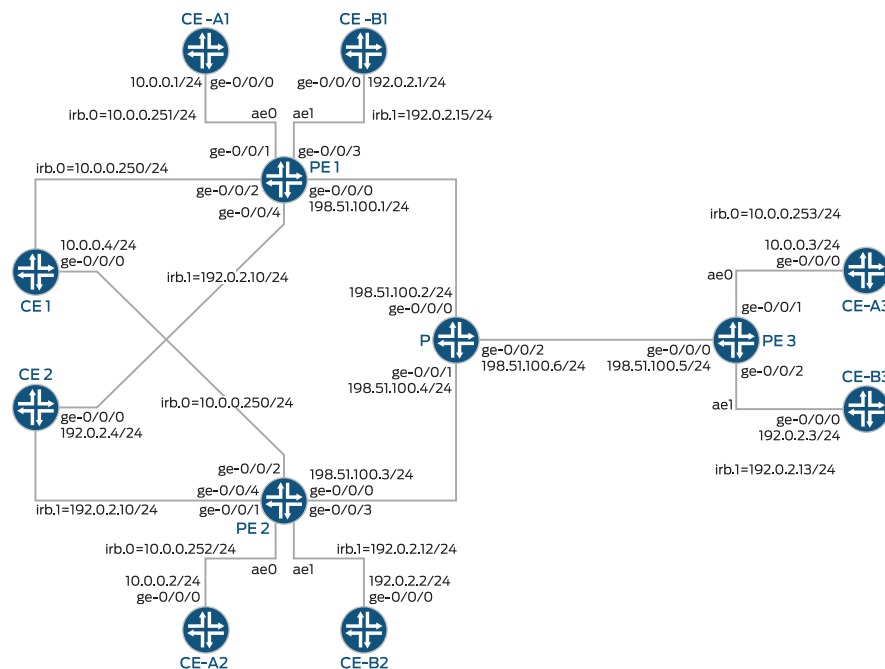
- DPCs provide support for EVPN in the active-standby mode of operation including support for the following:
 - a. EVPN instance (EVI)
 - b. Virtual switch (VS)
 - c. Integrated routing and bridging (IRB) interfaces
- DPCs intended for providing the EVPN active-standby support should be the CE device-facing line card. The PE device interfaces in the EVPN domain should use only MPC and MIC interfaces.

**NOTE:**

When configuring active-standby EVPN multihoming, be aware of the following limitations:

- An interface or ESI can be attached to more than one EVI, with a maximum limit of 200 EVIs per ESI.
- For an EVPN routing instance, only one logical interface per physical interface or ESI can be attached to an EVI.
- For a virtual switch routing instance, only one logical interface per physical interface or ESI can be configured under a bridge domain.
- All the PE routers in the network topology should be running Junos OS Release 14.1 or later releases, which are based on the EVPN draft-ietf-l2vpn-evpn-03. Junos OS releases prior to 14.1 support the older version of the EVPN draft, causing interoperability issues when Junos OS Release 14.1 and a previous release are running.

Figure 22: EVPN Active-Standby Multihoming



In Figure 22 on page 266, Routers PE1 and PE2 are provider edge (PE) routers connected to multihomed customer edge (CE) devices, Device CE1 and CE2. Router PE3 is a remote PE router connected to a single-homed customer site, and Router P is the provider router connected to Routers PE1, PE2, and PE3.

There are three routing instances running in the topology – ALPHA, BETA, and DELTA, with the virtual switch, EVPN, and VRF type of routing instance, respectively. All the PE

routers are connected to one single-homed CE device each for the ALPHA and BETA routing instances. Device CE1 belongs to the ALPHA routing instance, and Device CE2 belongs to the BETA routing instance.

For Router PE1, Device CE-A1 and Device CE-B1 are the single-homed CE devices for the routing instances ALPHA and BETA, respectively. In the same way, Device CE-A2 and Device CE-A3 belong to the ALPHA routing instance, and Device CE-B2 and Device CE-B3 belong to the BETA routing instances connected to Routers PE2 and PE3, respectively.

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.

```

CE1    set interfaces ge-0/0/0 vlan-tagging
        set interfaces ge-0/0/0 mac 00:00:00:00:00:04
        set interfaces ge-0/0/0 unit 0 vlan-id 100
        set interfaces ge-0/0/0 unit 0 family inet address 10.0.0.4/24
        set routing-options static route 0.0.0.0/0 next-hop 10.0.0.250

CE-A1   set chassis aggregated-devices ethernet device-count 1
        set interfaces ge-0/0/0 gigether-options 802.3ad ae0
        set interfaces ae0 vlan-tagging
        set interfaces ae0 mac 00:00:00:00:00:01
        set interfaces ae0 unit 0 vlan-id 100
        set interfaces ae0 unit 0 family inet address 10.0.0.1/24
        set routing-options static route 0.0.0.0/0 next-hop 10.0.0.251

CE-A2   set chassis aggregated-devices ethernet device-count 1
        set interfaces ge-0/0/0 gigether-options 802.3ad ae0
        set interfaces ae0 vlan-tagging
        set interfaces ae0 mac 00:00:00:00:00:02
        set interfaces ae0 unit 0 vlan-id 100
        set interfaces ae0 unit 0 family inet address 10.0.0.2/24
        set routing-options static route 0.0.0.0/0 next-hop 10.0.0.252

CE-A3   set chassis aggregated-devices ethernet device-count 1
        set interfaces ge-0/0/0 gigether-options 802.3ad ae0
        set interfaces ae0 vlan-tagging
        set interfaces ae0 mac 00:00:00:00:00:03
        set interfaces ae0 unit 0 vlan-id 100
        set interfaces ae0 unit 0 family inet address 10.0.0.3/24
        set routing-options static route 0.0.0.0/0 next-hop 10.0.0.253

CE2     set interfaces ge-0/0/0 vlan-tagging
        set interfaces ge-0/0/0 mac 00:00:00:00:00:04
        set interfaces ge-0/0/0 unit 0 vlan-id 300
        set interfaces ge-0/0/0 unit 0 family inet address 192.0.2.4/24
        set routing-options static route 0.0.0.0/0 next-hop 192.0.2.10

CE-B1   set chassis aggregated-devices ethernet device-count 1
        set interfaces ge-0/0/0 gigether-options 802.3ad ae0

```

```
set interfaces ae0 vlan-tagging
set interfaces ae0 mac 00:00:00:00:00:01
set interfaces ae0 unit 0 vlan-id 300
set interfaces ae0 unit 0 family inet address 192.0.2.1/24
set routing-options static route 0.0.0.0/0 next-hop 192.0.2.15

CE-B2  set chassis aggregated-devices ethernet device-count 1
set interfaces ge-0/0/0 gigether-options 802.3ad ae0
set interfaces ae0 vlan-tagging
set interfaces ae0 mac 00:00:00:00:00:02
set interfaces ae0 unit 0 vlan-id 300
set interfaces ae0 unit 0 family inet address 192.0.2.2/24
set routing-options static route 0.0.0.0/0 next-hop 192.0.2.12

CE-B3  set chassis aggregated-devices ethernet device-count 1
set interfaces ge-0/0/0 gigether-options 802.3ad ae0
set interfaces ae0 vlan-tagging
set interfaces ae0 mac 00:00:00:00:00:03
set interfaces ae0 unit 0 vlan-id 300
set interfaces ae0 unit 0 family inet address 192.0.2.3/24
set routing-options static route 0.0.0.0/0 next-hop 192.0.2.13

PE1    set interfaces ge-0/0/0 unit 0 family inet address 198.51.100.1/24
set interfaces ge-0/0/0 unit 0 family mpls
set interfaces ge-0/0/1 gigether-options 802.3ad ae0
set interfaces ge-0/0/2 vlan-tagging
set interfaces ge-0/0/2 encapsulation flexible-ethernet-services
set interfaces ge-0/0/2 unit 0 encapsulation vlan-bridge
set interfaces ge-0/0/2 unit 0 vlan-id 100
set interfaces ge-0/0/3 gigether-options 802.3ad ae1
set interfaces ge-0/0/4 vlan-tagging
set interfaces ge-0/0/4 encapsulation flexible-ethernet-services
set interfaces ge-0/0/4 esi 00:22:44:66:88:00:22:44:66:88
set interfaces ge-0/0/4 esi single-active
set interfaces ge-0/0/4 unit 0 encapsulation vlan-bridge
set interfaces ge-0/0/4 unit 0 vlan-id 300
set interfaces ae0 vlan-tagging
set interfaces ae0 encapsulation flexible-ethernet-services
set interfaces ae0 esi 00:11:22:33:44:55:66:77:88:99
set interfaces ae0 esi single-active
set interfaces ae0 unit 0 encapsulation vlan-bridge
set interfaces ae0 unit 0 vlan-id 100
set interfaces ae1 vlan-tagging
set interfaces ae1 encapsulation flexible-ethernet-services
set interfaces ae1 unit 0 encapsulation vlan-bridge
set interfaces ae1 unit 0 vlan-id 300
set interfaces irb unit 0 family inet address 10.0.0.250/24
set interfaces irb unit 0 family inet address 10.0.0.251/24
set interfaces irb unit 0 mac 00:11:22:33:44:55
set interfaces irb unit 1 family inet address 192.0.2.10/24
set interfaces irb unit 1 family inet address 192.0.2.15/24
set interfaces irb unit 1 mac 00:22:44:66:88:00
set interfaces lo0 unit 0 family inet address 10.255.0.1/32 primary
set interfaces lo0 unit 0 family inet address 10.255.0.1/32 preferred
set routing-options router-id 10.255.0.1
```



```

set routing-options autonomous-system 100
set routing-options forwarding-table chained-composite-next-hop ingress evpn
set protocols mpls interface lo0.0
set protocols mpls interface ge-0/0/0.0
set protocols bgp group EVPN-PE type internal
set protocols bgp group EVPN-PE local-address 10.255.0.1
set protocols bgp group EVPN-PE family evpn signaling
set protocols bgp group EVPN-PE neighbor 10.255.0.2
set protocols bgp group EVPN-PE neighbor 10.255.0.3
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-0/0/0.0
set protocols ldp interface ge-0/0/0.0
set protocols ldp interface lo0.0
set routing-instances ALPHA instance-type virtual-switch
set routing-instances ALPHA route-distinguisher 10.255.0.1:100
set routing-instances ALPHA vrf-target target:100:100
set routing-instances ALPHA protocols evpn extended-vlan-list 100
set routing-instances ALPHA bridge-domains ONE domain-type bridge
set routing-instances ALPHA bridge-domains ONE vlan-id 100
set routing-instances ALPHA bridge-domains ONE interface ae0.0
set routing-instances ALPHA bridge-domains ONE interface ge-0/0/2.0
set routing-instances ALPHA bridge-domains ONE routing-interface irb.0
set routing-instances BETA instance-type evpn
set routing-instances BETA vlan-id 300
set routing-instances BETA interface ge-0/0/4.0
set routing-instances BETA interface ae1.0
set routing-instances BETA routing-interface irb.1
set routing-instances BETA route-distinguisher 10.255.0.1:300
set routing-instances BETA vrf-target target:300:300
set routing-instances DELTA instance-type vrf
set routing-instances DELTA interface irb.0
set routing-instances DELTA interface irb.1
set routing-instances DELTA route-distinguisher 10.255.0.1:200
set routing-instances DELTA vrf-target target:200:200
set routing-instances DELTA vrf-table-label

```

```

PE2  set interfaces ge-0/0/0 unit 0 family inet address 198.51.100.3/24
      set interfaces ge-0/0/0 unit 0 family mpls
      set interfaces ge-0/0/1 gigether-options 802.3ad ae0
      set interfaces ge-0/0/2 vlan-tagging
      set interfaces ge-0/0/2 encapsulation flexible-ethernet-services
      set interfaces ge-0/0/2 unit 0 encapsulation vlan-bridge
      set interfaces ge-0/0/2 unit 0 vlan-id 100
      set interfaces ge-0/0/3 gigether-options 802.3ad ae1
      set interfaces ge-0/0/4 vlan-tagging
      set interfaces ge-0/0/4 encapsulation flexible-ethernet-services
      set interfaces ge-0/0/4 esi 00:22:44:66:88:00:22:44:66:88
      set interfaces ge-0/0/4 esi single-active
      set interfaces ge-0/0/4 unit 0 encapsulation vlan-bridge
      set interfaces ge-0/0/4 unit 0 vlan-id 300
      set interfaces ae0 vlan-tagging
      set interfaces ae0 encapsulation flexible-ethernet-services
      set interfaces ae0 esi 00:11:22:33:44:55:66:77:88:99
      set interfaces ae0 esi single-active
      set interfaces ae0 unit 0 encapsulation vlan-bridge
      set interfaces ae0 unit 0 vlan-id 100

```

```

set interfaces ae1 vlan-tagging
set interfaces ae1 encapsulation flexible-ethernet-services
set interfaces ae1 unit 0 encapsulation vlan-bridge
set interfaces ae1 unit 0 vlan-id 300
set interfaces irb unit 0 family inet address 10.0.0.250/24
set interfaces irb unit 0 family inet address 10.0.0.252/24
set interfaces irb unit 0 mac 00:11:22:33:44:55
set interfaces irb unit 1 family inet address 192.0.2.10/24
set interfaces irb unit 1 family inet address 192.0.2.12/24
set interfaces irb unit 1 mac 00:22:44:66:88:00
set interfaces lo0 unit 0 family inet address 10.255.0.2/32 primary
set interfaces lo0 unit 0 family inet address 10.255.0.2/32 preferred
set routing-options router-id 10.255.0.2
set routing-options autonomous-system 100
set routing-options forwarding-table chained-composite-next-hop ingress evpn
set protocols mpls interface lo0.0
set protocols mpls interface ge-0/0/0.0
set protocols bgp group EVPN-PE type internal
set protocols bgp group EVPN-PE local-address 10.255.0.2
set protocols bgp group EVPN-PE family evpn signaling
set protocols bgp group EVPN-PE neighbor 10.255.0.1
set protocols bgp group EVPN-PE neighbor 10.255.0.3
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-0/0/0.0
set protocols ldp interface ge-0/0/0.0
set protocols ldp interface lo0.0
set routing-instances ALPHA instance-type virtual-switch
set routing-instances ALPHA route-distinguisher 10.255.0.2:100
set routing-instances ALPHA vrf-target target:100:100
set routing-instances ALPHA protocols evpn extended-vlan-list 100
set routing-instances ALPHA bridge-domains ONE domain-type bridge
set routing-instances ALPHA bridge-domains ONE vlan-id 100
set routing-instances ALPHA bridge-domains ONE interface ae0.0
set routing-instances ALPHA bridge-domains ONE interface ge-0/0/2.0
set routing-instances ALPHA bridge-domains ONE routing-interface irb.0
set routing-instances BETA instance-type evpn
set routing-instances BETA vlan-id 300
set routing-instances BETA interface ge-0/0/4.0
set routing-instances BETA interface ae1.0
set routing-instances BETA routing-interface irb.1
set routing-instances BETA route-distinguisher 10.255.0.2:300
set routing-instances BETA vrf-target target:300:300
set routing-instances DELTA instance-type vrf
set routing-instances DELTA interface irb.0
set routing-instances DELTA interface irb.1
set routing-instances DELTA route-distinguisher 10.255.0.2:200
set routing-instances DELTA vrf-target target:200:200
set routing-instances DELTA vrf-table-label

```

```

PE3 set interfaces ge-0/0/0 unit 0 family inet address 198.51.100.5/24
set interfaces ge-0/0/0 unit 0 family mpls
set interfaces ge-0/0/1 gigether-options 802.3ad ae0
set interfaces ge-0/0/2 gigether-options 802.3ad ae1
set interfaces ae0 vlan-tagging
set interfaces ae0 encapsulation flexible-ethernet-services
set interfaces ae0 unit 0 encapsulation vlan-bridge

```

```

set interfaces ae0 unit 0 vlan-id 100
set interfaces ae1 vlan-tagging
set interfaces ae1 encapsulation flexible-ethernet-services
set interfaces ae1 unit 0 encapsulation vlan-bridge
set interfaces ae1 unit 0 vlan-id 300
set interfaces irb unit 0 family inet address 10.0.0.253/24
set interfaces irb unit 1 family inet address 192.0.2.13/24
set interfaces lo0 unit 0 family inet address 10.255.0.3/32 primary
set interfaces lo0 unit 0 family inet address 10.255.0.3/32 preferred
set routing-options router-id 10.255.0.3
set routing-options autonomous-system 100
set routing-options forwarding-table chained-composite-next-hop ingress evpn
set protocols mpls interface lo0.0
set protocols mpls interface ge-0/0/0.0
set protocols bgp group EVPN-PE type internal
set protocols bgp group EVPN-PE local-address 10.255.0.3
set protocols bgp group EVPN-PE family evpn signaling
set protocols bgp group EVPN-PE neighbor 10.255.0.1
set protocols bgp group EVPN-PE neighbor 10.255.0.2
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-0/0/0.0
set protocols ldp interface ge-0/0/0.0
set protocols ldp interface lo0.0
set routing-instances ALPHA instance-type virtual-switch
set routing-instances ALPHA route-distinguisher 10.255.0.3:100
set routing-instances ALPHA vrf-target target:100:100
set routing-instances ALPHA protocols evpn extended-vlan-list 100
set routing-instances ALPHA bridge-domains ONE domain-type bridge
set routing-instances ALPHA bridge-domains ONE vlan-id 100
set routing-instances ALPHA bridge-domains ONE interface ae0.0
set routing-instances ALPHA bridge-domains ONE routing-interface irb.0
set routing-instances BETA instance-type evpn
set routing-instances BETA vlan-id 300
set routing-instances BETA interface ae1.0
set routing-instances BETA routing-interface irb.1
set routing-instances BETA route-distinguisher 10.255.0.3:300
set routing-instances BETA vrf-target target:300:300
set routing-instances DELTA instance-type vrf
set routing-instances DELTA interface irb.0
set routing-instances DELTA interface irb.1
set routing-instances DELTA route-distinguisher 10.255.0.3:200
set routing-instances DELTA vrf-target target:200:200
set routing-instances DELTA vrf-table-label

```

```

P set interfaces ge-0/0/0 unit 0 family inet address 198.51.100.2/24
set interfaces ge-0/0/0 unit 0 family mpls
set interfaces ge-0/0/1 unit 0 family inet address 198.51.100.4/24
set interfaces ge-0/0/1 unit 0 family mpls
set interfaces ge-0/0/2 unit 0 family inet address 198.51.100.6/24
set interfaces ge-0/0/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.0.4/32 primary
set interfaces lo0 unit 0 family inet address 10.255.0.4/32 preferred
set routing-options router-id 10.255.0.4
set protocols mpls interface lo0.0
set protocols mpls interface ge-0/0/0.0
set protocols mpls interface ge-0/0/1.0

```

```

set protocols mpls interface ge-0/0/2.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-0/0/1.0
set protocols ospf area 0.0.0.0 interface ge-0/0/2.0
set protocols ospf area 0.0.0.0 interface ge-0/0/0.0
set protocols ldp interface ge-0/0/0.0
set protocols ldp interface ge-0/0/1.0
set protocols ldp interface ge-0/0/2.0
set protocols ldp interface lo0.0

```

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 Router PE1:



NOTE: Repeat this procedure for Router PE2 after modifying the appropriate interface names, addresses, and other parameters.

1. Configure Router PE1 interfaces.

[edit interfaces]

```

user@PE1# set ge-0/0/0 unit 0 family inet address 198.51.100.1/24
user@PE1# set ge-0/0/0 unit 0 family mpls

```

```

user@PE1# set ge-0/0/1 gigether-options 802.3ad ae0

```

```

user@PE1# set ge-0/0/2 vlan-tagging
user@PE1# set ge-0/0/2 encapsulation flexible-ethernet-services
user@PE1# set ge-0/0/2 unit 0 encapsulation vlan-bridge
user@PE1# set ge-0/0/2 unit 0 vlan-id 100

```

```

user@PE1# set ge-0/0/3 gigether-options 802.3ad ae1

```

```

user@PE1# set ge-0/0/4 vlan-tagging
user@PE1# set ge-0/0/4 encapsulation flexible-ethernet-services
user@PE1# set ge-0/0/4 esi 00:22:44:66:88:00:22:44:66:88
user@PE1# set ge-0/0/4 esi single-active
user@PE1# set ge-0/0/4 unit 0 encapsulation vlan-bridge
user@PE1# set ge-0/0/4 unit 0 vlan-id 300

```

```

user@PE1# set ae0 vlan-tagging
user@PE1# set ae0 encapsulation flexible-ethernet-services
user@PE1# set ae0 esi 00:11:22:33:44:55:66:77:88:99
user@PE1# set ae0 esi single-active
user@PE1# set ae0 unit 0 encapsulation vlan-bridge
user@PE1# set ae0 unit 0 vlan-id 100

```

```

user@PE1# set ae1 vlan-tagging
user@PE1# set ae1 encapsulation flexible-ethernet-services

```

```
user@PE1# set ae1 unit 0 encapsulation vlan-bridge
user@PE1# set ae1 unit 0 vlan-id 300
```

```
user@PE1# set irb unit 0 family inet address 10.0.0.250/24
user@PE1# set irb unit 0 family inet address 10.0.0.251/24
user@PE1# set irb unit 0 mac 00:11:22:33:44:55
user@PE1# set irb unit 1 family inet address 192.0.2.10/24
user@PE1# set irb unit 1 family inet address 192.0.2.15/24
user@PE1# set irb unit 1 mac 00:22:44:66:88:00
```

```
user@PE1# set lo0 unit 0 family inet address 10.255.0.1/32 primary
user@PE1# set lo0 unit 0 family inet address 10.255.0.1/32 preferred
```

2. Configure the loopback address of Router PE1 as the router ID.

```
[edit routing-options]
user@PE1# set router-id 10.255.0.1
```

3. Set the autonomous system number for Router PE1.

```
[edit routing-options]
user@PE1# set autonomous-system 100
```

4. Enable chained composite next hop for the EVPN.

```
[edit routing-options]
user@PE1# set forwarding-table chained-composite-next-hop ingress evpn
```

5. Enable MPLS on the loopback interface of Router PE1 and the interface connecting PE1 to Router P.

```
[edit protocols]
user@PE1# set mpls interface lo0.0
user@PE1# set mpls interface ge-0/0/0.0
```

6. Configure the BGP group for Router PE1.

```
[edit protocols]
user@PE1# set bgp group EVPN-PE type internal
```

7. Assign local and neighbor addresses to the EVPN-PE BGP group for Router PE1 to peer with Routers PE2 and PE3.

```
[edit protocols]
user@PE1# set bgp group EVPN-PE local-address 10.255.0.1
user@PE1# set bgp group EVPN-PE neighbor 10.255.0.2
user@PE1# set bgp group EVPN-PE neighbor 10.255.0.3
```

8. Include the EVPN signaling Network Layer Reachability Information (NLRI) to the EVPN-PE group.

```
[edit protocols]
user@PE1# set bgp group EVPN-PE family evpn signaling
```

9. Configure OSPF on the loopback interface of Router PE1 and the interface connecting PE1 to Router P.

```
[edit protocols]
user@PE1# set ospf area 0.0.0.0 interface lo0.0 passive
user@PE1# set ospf area 0.0.0.0 interface ge-0/0/0.0
```

10. Enable LDP on the loopback interface of Router PE1 and the interface connecting PE1 to Router P.

[edit protocols]
user@PE1# set ldp interface lo0.0
user@PE1# set ldp interface ge-0/0/0.0
11. Configure the virtual switch routing instance – ALPHA.

[edit routing-instances]
user@PE1# set ALPHA instance-type virtual-switch
12. Configure the extended VLAN list for the ALPHA routing instance.

[edit routing-instances]
user@PE1# set ALPHA protocols evpn extended-vlan-list 100
13. Set the type for the bridging domain in the ALPHA routing instance.

[edit routing-instances]
user@PE1# set ALPHA bridge-domains ONE domain-type bridge
14. Set the VLAN for the bridging domain in the ALPHA routing instance.

[edit routing-instances]
user@PE1# set ALPHA bridge-domains ONE vlan-id 100
15. Configure the interface names for the ALPHA routing instance.

[edit routing-instances]
user@PE1# set ALPHA bridge-domains ONE interface ae0.0
user@PE1# set ALPHA bridge-domains ONE interface ge-0/0/2.0
user@PE1# set ALPHA bridge-domains ONE routing-interface irb.0
16. Configure the route distinguisher for the ALPHA routing instance.

[edit routing-instances]
user@PE1# set ALPHA route-distinguisher 10.255.0.1:100
17. Configure the VPN routing and forwarding (VRF) target community for the ALPHA routing instance.

[edit routing-instances]
user@PE1# set ALPHA vrf-target target:100:100
18. Configure the EVPN routing instance – BETA.

[edit routing-instances]
user@PE1# set BETA instance-type evpn
19. Set the VLAN identifier for the bridging domain in the BETA routing instance.

[edit routing-instances]
user@PE1# set BETA vlan-id 300
20. Configure the interface names for the BETA routing instance.

[edit routing-instances]
user@PE1# set BETA interface ge-0/0/4.0
user@PE1# set BETA interface ae1.0
user@PE1# set BETA routing-interface irb.1
21. Configure the route distinguisher for the BETA routing instance.

```
[edit routing-instances]
user@PE1# set BETA route-distinguisher 10.255.0.1:300
```

22. Configure the VPN routing and forwarding (VRF) target community for the BETA routing instance.

```
[edit routing-instances]
user@PE1# set BETA vrf-target target:300:300
```

23. Configure the VRF routing instance – DELTA.

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

24. Configure the interface names for the DELTA routing instance.

```
[edit routing-instances]
user@PE1# set DELTA interface irb.0
user@PE1# set DELTA interface irb.1
```

25. Configure the route distinguisher for the DELTA routing instance.

```
[edit routing-instances]
user@PE1# set DELTA route-distinguisher 10.255.0.1:200
```

26. Configure the VPN routing and forwarding (VRF) target community for the DELTA routing instance.

```
[edit routing-instances]
user@PE1# set DELTA vrf-target target:200:200
user@PE1# set DELTA vrf-table-label
```

Results

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

```
user@PE1# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet {
      address 198.51.100.1/24;
    }
    family mpls;
  }
}
ge-0/0/1 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-0/0/2 {
  vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 0 {
    encapsulation vlan-bridge;
```

```
        vlan-id 100;
    }
}
ge-0/0/3 {
    gigether-options {
        802.3ad ae1;
    }
}
ge-0/0/4 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    esi {
        00:22:44:66:88:00:22:44:66:88;
        single-active;
    }
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id 300;
    }
}
ae0 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    esi {
        00:11:22:33:44:55:66:77:88:99;
        single-active;
    }
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id 100;
    }
}
ae1 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id 300;
    }
}
irb {
    unit 0 {
        family inet {
            address 10.0.0.250/24;
            address 10.0.0.251/24;
        }
        mac 00:11:22:33:44:55;
    }
    unit 1 {
        family inet {
            address 192.0.2.10/24;
            address 192.0.2.15/24;
        }
        mac 00:22:44:66:88:00;
    }
}
```



```

lo0 {
  unit 0 {
    family inet {
      address 10.255.0.1/32 {
        primary;
        preferred;
      }
    }
  }
}

user@PE1# show routing-options
router-id 10.255.0.1;
autonomous-system 100;
forwarding-table {
  chained-composite-next-hop {
    ingress {
      evpn;
    }
  }
}

user@PE1# show protocols
mpls {
  interface lo0.0;
  interface ge-0/0/0.0;
}
bgp {
  group EVPN-PE {
    type internal;
    local-address 10.255.0.1;
    family evpn {
      signaling;
    }
    neighbor 10.255.0.2;
    neighbor 10.255.0.3;
  }
}
ospf {
  area 0.0.0.0 {
    interface lo0.0 {
      passive;
    }
    interface ge-0/0/0.0;
  }
}
ldp {
  interface ge-0/0/0.0;
  interface lo0.0;
}

user@PE1# show routing-instances
ALPHA {
  instance-type virtual-switch;
  route-distinguisher 10.255.0.1:100;
  vrf-target target:100:100;
  protocols {

```

```
    evpn {
        extended-vlan-list 100;
    }
}
bridge-domains {
    ONE {
        domain-type bridge;
        vlan-id 100;
        interface ae0.0;
        interface ge-0/0/2.0;
        routing-interface irb.0;
    }
}
BETA {
    instance-type evpn;
    vlan-id 300;
    interface ge-0/0/4.0;
    interface ae1.0;
    routing-interface irb.1;
    route-distinguisher 10.255.0.1:300;
    vrf-target target:300:300;
}
DELTA {
    instance-type vrf;
    interface irb.0;
    interface irb.1;
    route-distinguisher 10.255.0.1:200;
    vrf-target target:200:200;
    vrf-table-label;
}
```

Verification

Confirm that the configuration is working properly in the following different areas on all the PE routers, where Router PE1 is the designated forwarder (DF), Router PE2 is the non-DF, and Router PE3 is the remote PE:

- a. EVPN routing instance configuration
 - b. EVPN multihoming routes
 - c. DF election process
 - d. IRB and virtual switch routing instance configuration
 - e. Host route entries
- [Verifying the EVPN Instance Status on page 279](#)
 - [Verifying the Autodiscovery Routes per Ethernet Segment on page 283](#)
 - [Verifying the Ethernet Segment Route on page 288](#)
 - [Verifying the DF Status on page 289](#)
 - [Verifying the BDF Status on page 289](#)
 - [Verifying Remote IRB MAC on page 289](#)

- [Verifying Remote IRB and Host IP on page 290](#)
- [Verifying ARP Table on page 293](#)
- [Verifying Bridge ARP Table on page 293](#)
- [Verifying Bridge MAC Table on page 294](#)

Verifying the EVPN Instance Status

Purpose Verify the EVPN routing instances and their status.

Router PE1 Action

From operational mode, run the **show evpn instance extensive** command.

```

user@PE1> show evpn instance extensive
Instance: ALPHA
  Route Distinguisher: 10.255.0.1:100
  Per-instance MAC route label: 300144
  Per-instance multicast route label: 300160
  MAC database status
    Total MAC addresses:          Local Remote
    Default gateway MAC addresses: 1      2
  Number of local interfaces: 2 (2 up)
    Interface name  ESI
    ae0.0           00:11:22:33:44:55:66:77:88:99  single-active
    ge-0/0/2.0      00:00:00:00:00:00:00:00:00:00  single-homed
  Number of IRB interfaces: 1 (1 up)
    Interface name  L3 context
    irb.0           DELTA
  Number of neighbors: 2
    10.255.0.2
      Received routes
        MAC address advertisement:          2
        MAC+IP address advertisement:       3
        Inclusive multicast:                1
        Ethernet auto-discovery:            1
    10.255.0.3
      Received routes
        MAC address advertisement:          2
        MAC+IP address advertisement:       2
        Inclusive multicast:                1
        Ethernet auto-discovery:            0
  Number of ethernet segments: 1
    ESI: 00:11:22:33:44:55:66:77:88:99
    Designated forwarder: 10.255.0.1
    Backup forwarder: 10.255.0.2

Instance: BETA
  Route Distinguisher: 10.255.0.1:300
  VLAN ID: 300
  Per-instance MAC route label: 300176
  Per-instance multicast route label: 300192
  MAC database status
    Total MAC addresses:          Local Remote
    Default gateway MAC addresses: 1      2
  Number of local interfaces: 2 (2 up)
    Interface name  ESI
    ae1.0           00:00:00:00:00:00:00:00:00:00  single-homed
    ge-0/0/4.0      00:22:44:66:88:00:22:44:66:88  single-active
  
```

```

Number of IRB interfaces: 1 (1 up)
Interface name  L3 context
irb.1          DELTA
Number of neighbors: 2
10.255.0.2
  Received routes
    MAC address advertisement:      2
    MAC+IP address advertisement:   3
    Inclusive multicast:            1
    Ethernet auto-discovery:        1
10.255.0.3
  Received routes
    MAC address advertisement:      2
    MAC+IP address advertisement:   2
    Inclusive multicast:            1
    Ethernet auto-discovery:        0
Number of ethernet segments: 1
ESI: 00:22:44:66:88:00:22:44:66:88
  Designated forwarder: 10.255.0.1
  Backup forwarder: 10.255.0.2

Instance: __default_evpn__
Route Distinguisher: 10.255.0.1:0
VLAN ID: 0
Per-instance MAC route label: 300208
Per-instance multicast route label: 300224
MAC database status
Total MAC addresses:      Local Remote
Default gateway MAC addresses: 0      0
Number of local interfaces: 0 (0 up)
Number of IRB interfaces: 0 (0 up)
Number of neighbors: 1
10.255.0.2
  Received routes
    Ethernet auto-discovery:      0
    Ethernet Segment:             2
Number of ethernet segments: 0

```

Router PE2

From operational mode, run the **show evpn instance extensive** command.

```

user@PE2> show evpn instance extensive
Instance: ALPHA
Route Distinguisher: 10.255.0.2:100
Per-instance MAC route label: 300208
Per-instance multicast route label: 300224
MAC database status
Total MAC addresses:      Local Remote
Default gateway MAC addresses: 1      2
Number of local interfaces: 2 (2 up)
Interface name  ESI                               Mode          SH label
ae0.0          00:11:22:33:44:55:66:77:88:99  single-active
ge-0/0/2.0     00:00:00:00:00:00:00:00:00:00  single-homed
Number of IRB interfaces: 1 (1 up)
Interface name  L3 context
irb.0          DELTA
Number of neighbors: 2
10.255.0.1
  Received routes
    MAC address advertisement:      3

```

```

    MAC+IP address advertisement:      4
    Inclusive multicast:                1
    Ethernet auto-discovery:           1
10.255.0.3
    Received routes
    MAC address advertisement:          2
    MAC+IP address advertisement:       2
    Inclusive multicast:                1
    Ethernet auto-discovery:            0
Number of ethernet segments: 1
ESI: 00:11:22:33:44:55:66:77:88:99
    Designated forwarder: 10.255.0.1
    Backup forwarder: 10.255.0.2

Instance: BETA
Route Distinguisher: 10.255.0.2:300
VLAN ID: 300
Per-instance MAC route label: 300240
Per-instance multicast route label: 300256
MAC database status          Local Remote
Total MAC addresses:         2       5
Default gateway MAC addresses: 1       2
Number of local interfaces: 2 (2 up)
Interface name  ESI                               Mode          SH label
ae1.0           00:00:00:00:00:00:00:00:00:00    single-homed
ge-0/0/4.0      00:22:44:66:88:00:22:44:66:88    single-active
Number of IRB interfaces: 1 (1 up)
Interface name  L3 context
irb.1           DELTA
Number of neighbors: 2
10.255.0.1
    Received routes
    MAC address advertisement:          3
    MAC+IP address advertisement:       4
    Inclusive multicast:                1
    Ethernet auto-discovery:            1
10.255.0.3
    Received routes
    MAC address advertisement:          2
    MAC+IP address advertisement:       2
    Inclusive multicast:                1
    Ethernet auto-discovery:            0
Number of ethernet segments: 1
ESI: 00:22:44:66:88:00:22:44:66:88
    Designated forwarder: 10.255.0.1
    Backup forwarder: 10.255.0.2

Instance: __default_evpn__
Route Distinguisher: 10.255.0.2:0
VLAN ID: 0
Per-instance MAC route label: 300272
Per-instance multicast route label: 300288
MAC database status          Local Remote
Total MAC addresses:         0       0
Default gateway MAC addresses: 0       0
Number of local interfaces: 0 (0 up)
Number of IRB interfaces: 0 (0 up)
Number of neighbors: 1
10.255.0.1
    Received routes
    Ethernet auto-discovery:            0

```

Ethernet Segment: 2
 Number of ethernet segments: 0

Router PE3

From operational mode, run the **show evpn instance extensive** command.

```
user@PE3> show evpn instance extensive
Instance: ALPHA
  Route Distinguisher: 10.255.0.3:100
  Per-instance MAC route label: 299776
  Per-instance multicast route label: 299792
  MAC database status
    Total MAC addresses: 2 4
    Default gateway MAC addresses: 1 1
  Number of local interfaces: 1 (1 up)
    Interface name ESI Mode SH label
    ae0.0 00:00:00:00:00:00:00:00:00 single-homed
  Number of IRB interfaces: 1 (1 up)
    Interface name L3 context
    irb.0 DELTA
  Number of neighbors: 2
    10.255.0.1
      Received routes
        MAC address advertisement: 3
        MAC+IP address advertisement: 4
        Inclusive multicast: 1
        Ethernet auto-discovery: 1
    10.255.0.2
      Received routes
        MAC address advertisement: 2
        MAC+IP address advertisement: 3
        Inclusive multicast: 1
        Ethernet auto-discovery: 1
  Number of ethernet segments: 0

Instance: BETA
  Route Distinguisher: 10.255.0.3:300
  VLAN ID: 300
  Per-instance MAC route label: 299808
  Per-instance multicast route label: 299824
  MAC database status
    Total MAC addresses: 2 4
    Default gateway MAC addresses: 1 1
  Number of local interfaces: 1 (1 up)
    Interface name ESI Mode SH label
    ae1.0 00:00:00:00:00:00:00:00:00 single-homed
  Number of IRB interfaces: 1 (1 up)
    Interface name L3 context
    irb.1 DELTA
  Number of neighbors: 2
    10.255.0.1
      Received routes
        MAC address advertisement: 3
        MAC+IP address advertisement: 4
        Inclusive multicast: 1
        Ethernet auto-discovery: 1
    10.255.0.2
      Received routes
        MAC address advertisement: 2
        MAC+IP address advertisement: 3
```

```

    Inclusive multicast: 1
    Ethernet auto-discovery: 1
    Number of ethernet segments: 0

Instance: __default_evpn__
Route Distinguisher: 10.255.0.3:0
VLAN ID: 0
Per-instance MAC route label: 299840
Per-instance multicast route label: 299856
MAC database status
    Total MAC addresses: 0 0
    Default gateway MAC addresses: 0 0
Number of local interfaces: 0 (0 up)
Number of IRB interfaces: 0 (0 up)
Number of neighbors: 0
Number of ethernet segments: 0

```

Meaning The output provides the following information:

- List of EVPN and virtual switch routing instances.
- Mode of operation of each interface
- Neighbors of each routing instance.
- Number of different routes received from each neighbor.
- ESI attached to each routing instance.
- Number of Ethernet segments on each routing instance.
- DF election roles for each ESI in an EVI.
- VLAN ID and MAC labels for each routing instance.
- IRB interface details
- Number of default gateway MAC addresses received for the virtual switch routing instance (ALPHA).

Verifying the Autodiscovery Routes per Ethernet Segment

Purpose Verify that the autodiscovery routes per Ethernet segment are received.

Router PE1 Action

From operational mode, run the **show route table ALPHA.evpn.0** command.

```

user@PE1> show route table ALPHA.evpn.0
ALPHA.evpn.0: 20 destinations, 20 routes (20 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1:10.255.0.2:0::112233445566778899::0/304
    *[BGP/170] 2d 23:51:27, localpref 100, from 10.255.0.2
    AS path: I, validation-state: unverified
    > to 198.51.100.2 via ge-0/0/0.0, Push 299808
2:10.255.0.1:100::100::00:00:00:00:00:01/304
    *[EVPN/170] 2d 23:52:22
    Indirect

```

```

2:10.255.0.1:100::100::00:00:00:00:00:04/304
    *[EVPN/170] 2d 23:52:24
    Indirect
2:10.255.0.1:100::100::00:11:22:33:44:55/304
    *[EVPN/170] 2d 23:53:32
    Indirect
2:10.255.0.2:100::100::00:00:00:00:00:02/304
    *[BGP/170] 2d 23:51:27, localpref 100, from 10.255.0.2
    AS path: I, validation-state: unverified
    > to 198.51.100.2 via ge-0/0/0.0, Push 299808
2:10.255.0.2:100::100::00:11:22:33:44:55/304
    *[BGP/170] 2d 23:51:27, localpref 100, from 10.255.0.2
    AS path: I, validation-state: unverified
    > to 198.51.100.2 via ge-0/0/0.0, Push 299808
2:10.255.0.3:100::100::00:00:00:00:00:03/304
    *[BGP/170] 2d 23:39:04, localpref 100, from 10.255.0.3
    AS path: I, validation-state: unverified
    > to 198.51.100.2 via ge-0/0/0.0, Push 299824
2:10.255.0.3:100::100::00:05:86:71:b3:f0/304
    *[BGP/170] 2d 23:39:24, localpref 100, from 10.255.0.3
    AS path: I, validation-state: unverified
    > to 198.51.100.2 via ge-0/0/0.0, Push 299824
2:10.255.0.1:100::100::00:00:00:00:00:01::10.0.0.1/304
    *[EVPN/170] 2d 23:52:22
    Indirect
2:10.255.0.1:100::100::00:00:00:00:00:04::10.0.0.4/304
    *[EVPN/170] 2d 23:52:24
    Indirect
2:10.255.0.1:100::100::00:11:22:33:44:55::10.0.0.250/304
    *[EVPN/170] 2d 23:53:32
    Indirect
2:10.255.0.1:100::100::00:11:22:33:44:55::10.0.0.251/304
    *[EVPN/170] 2d 23:53:32
    Indirect
2:10.255.0.2:100::100::00:00:00:00:00:02::10.0.0.2/304
    *[BGP/170] 2d 23:51:27, localpref 100, from 10.255.0.2
    AS path: I, validation-state: unverified
    > to 198.51.100.2 via ge-0/0/0.0, Push 299808
2:10.255.0.2:100::100::00:11:22:33:44:55::10.0.0.250/304
    *[BGP/170] 2d 23:51:27, localpref 100, from 10.255.0.2
    AS path: I, validation-state: unverified
    > to 198.51.100.2 via ge-0/0/0.0, Push 299808
2:10.255.0.2:100::100::00:11:22:33:44:55::10.0.0.252/304
    *[BGP/170] 2d 23:51:27, localpref 100, from 10.255.0.2
    AS path: I, validation-state: unverified
    > to 198.51.100.2 via ge-0/0/0.0, Push 299808
2:10.255.0.3:100::100::00:00:00:00:00:03::10.0.0.3/304
    *[BGP/170] 2d 23:39:04, localpref 100, from 10.255.0.3
    AS path: I, validation-state: unverified
    > to 198.51.100.2 via ge-0/0/0.0, Push 299824
2:10.255.0.3:100::100::00:05:86:71:b3:f0::10.0.0.253/304
    *[BGP/170] 2d 23:39:24, localpref 100, from 10.255.0.3
    AS path: I, validation-state: unverified
    > to 198.51.100.2 via ge-0/0/0.0, Push 299824
3:10.255.0.1:100::10.255.0.1/304
    *[EVPN/170] 2d 23:52:33
    Indirect
3:10.255.0.2:100::10.255.0.2/304
    *[BGP/170] 2d 23:51:27, localpref 100, from 10.255.0.2
    AS path: I, validation-state: unverified
    > to 198.51.100.2 via ge-0/0/0.0, Push 299808

```



```

3:10.255.0.3:100::100::10.255.0.3/304
  * [BGP/170] 2d 23:39:24, localpref 100, from 10.255.0.3
    AS path: I, validation-state: unverified
    > to 198.51.100.2 via ge-0/0/0.0, Push 299824

```

Router PE2

From operational mode, run the **show route table ALPHA.evpn.0** command.

```

user@PE2> show show route table ALPHA.evpn.0
ALPHA.evpn.0: 20 destinations, 20 routes (20 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

```

```

1:10.255.0.1:0::112233445566778899::0/304
  * [BGP/170] 10:46:04, localpref 100, from 10.255.0.1
    AS path: I, validation-state: unverified
    > to 198.51.100.4 via ge-0/0/0.0, Push 299776
2:10.255.0.1:100::100::00:00:00:00:00:01/304
  * [BGP/170] 10:43:51, localpref 100, from 10.255.0.1
    AS path: I, validation-state: unverified
    > to 198.51.100.4 via ge-0/0/0.0, Push 299776
2:10.255.0.1:100::100::00:00:00:00:00:04/304
  * [BGP/170] 10:45:06, localpref 100, from 10.255.0.1
    AS path: I, validation-state: unverified
    > to 198.51.100.4 via ge-0/0/0.0, Push 299776
2:10.255.0.1:100::100::00:11:22:33:44:55/304
  * [BGP/170] 10:46:04, localpref 100, from 10.255.0.1
    AS path: I, validation-state: unverified
    > to 198.51.100.4 via ge-0/0/0.0, Push 299776
2:10.255.0.2:100::100::00:00:00:00:00:02/304
  * [EVPN/170] 10:43:48
    Indirect
2:10.255.0.2:100::100::00:11:22:33:44:55/304
  * [EVPN/170] 10:46:04
    Indirect
2:10.255.0.3:100::100::00:00:00:00:00:03/304
  * [BGP/170] 10:46:04, localpref 100, from 10.255.0.3
    AS path: I, validation-state: unverified
    > to 198.51.100.4 via ge-0/0/0.0, Push 299792
2:10.255.0.3:100::100::00:05:86:71:79:f0/304
  * [BGP/170] 10:46:04, localpref 100, from 10.255.0.3
    AS path: I, validation-state: unverified
    > to 198.51.100.4 via ge-0/0/0.0, Push 299792
2:10.255.0.1:100::100::00:00:00:00:00:01::10.0.0.1/304
  * [BGP/170] 10:41:52, localpref 100, from 10.255.0.1
    AS path: I, validation-state: unverified
    > to 198.51.100.4 via ge-0/0/0.0, Push 299776
2:10.255.0.1:100::100::00:00:00:00:00:04::10.0.0.4/304
  * [BGP/170] 10:45:06, localpref 100, from 10.255.0.1
    AS path: I, validation-state: unverified
    > to 198.51.100.4 via ge-0/0/0.0, Push 299776
2:10.255.0.1:100::100::00:11:22:33:44:55::10.0.0.250/304
  * [BGP/170] 10:46:04, localpref 100, from 10.255.0.1
    AS path: I, validation-state: unverified
    > to 198.51.100.4 via ge-0/0/0.0, Push 299776
2:10.255.0.1:100::100::00:11:22:33:44:55::10.0.0.251/304
  * [BGP/170] 10:46:04, localpref 100, from 10.255.0.1
    AS path: I, validation-state: unverified
    > to 198.51.100.4 via ge-0/0/0.0, Push 299776
2:10.255.0.2:100::100::00:00:00:00:00:02::10.0.0.2/304
  * [EVPN/170] 10:40:25

```

```

Indirect
2:10.255.0.2:100::100::00:11:22:33:44:55::10.0.0.250/304
*[EVPN/170] 10:46:04
Indirect
2:10.255.0.2:100::100::00:11:22:33:44:55::10.0.0.252/304
*[EVPN/170] 10:46:04
Indirect
2:10.255.0.3:100::100::00:00:00:00:00:03::10.0.0.3/304
*[BGP/170] 10:46:04, localpref 100, from 10.255.0.3
AS path: I, validation-state: unverified
> to 198.51.100.4 via ge-0/0/0.0, Push 299792
2:10.255.0.3:100::100::00:05:86:71:79:f0::10.0.0.253/304
*[BGP/170] 10:46:04, localpref 100, from 10.255.0.3
AS path: I, validation-state: unverified
> to 198.51.100.4 via ge-0/0/0.0, Push 299792
3:10.255.0.1:100::100::10.255.0.1/304
*[BGP/170] 10:46:04, localpref 100, from 10.255.0.1
AS path: I, validation-state: unverified
> to 198.51.100.4 via ge-0/0/0.0, Push 299776
3:10.255.0.2:100::100::10.255.0.2/304
*[EVPN/170] 10:46:04
Indirect
3:10.255.0.3:100::100::10.255.0.3/304
*[BGP/170] 10:46:04, localpref 100, from 10.255.0.3
AS path: I, validation-state: unverified
> to 198.51.100.4 via ge-0/0/0.0, Push 299792

```

Router PE3

From operational mode, run the **show route table ALPHA.evpn.0** command.

```

user@PE3> show route table ALPHA.evpn.0
ALPHA.evpn.0: 21 destinations, 21 routes (21 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1:10.255.0.1:0::112233445566778899::0/304
*[BGP/170] 10:47:43, localpref 100, from 10.255.0.1
AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299776
1:10.255.0.2:0::112233445566778899::0/304
*[BGP/170] 10:47:34, localpref 100, from 10.255.0.2
AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299808
2:10.255.0.1:100::100::00:00:00:00:00:01/304
*[BGP/170] 10:45:21, localpref 100, from 10.255.0.1
AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299776
2:10.255.0.1:100::100::00:00:00:00:00:04/304
*[BGP/170] 10:46:36, localpref 100, from 10.255.0.1
AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299776
2:10.255.0.1:100::100::00:11:22:33:44:55/304
*[BGP/170] 10:47:43, localpref 100, from 10.255.0.1
AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299776
2:10.255.0.2:100::100::00:00:00:00:00:02/304
*[BGP/170] 10:45:18, localpref 100, from 10.255.0.2
AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299808
2:10.255.0.2:100::100::00:11:22:33:44:55/304
*[BGP/170] 10:47:34, localpref 100, from 10.255.0.2

```

```

AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299808
2:10.255.0.3:100::100::00:00:00:00:03/304
*[EVPN/170] 10:59:05
Indirect
2:10.255.0.3:100::100::00:05:86:71:79:f0/304
*[EVPN/170] 11:00:23
Indirect
2:10.255.0.1:100::100::00:00:00:00:01::10.0.0.1/304
*[BGP/170] 10:43:22, localpref 100, from 10.255.0.1
AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299776
2:10.255.0.1:100::100::00:00:00:00:04::10.0.0.4/304
*[BGP/170] 10:46:36, localpref 100, from 10.255.0.1
AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299776
2:10.255.0.1:100::100::00:11:22:33:44:55::10.0.0.250/304
*[BGP/170] 10:47:43, localpref 100, from 10.255.0.1
AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299776
2:10.255.0.1:100::100::00:11:22:33:44:55::10.0.0.251/304
*[BGP/170] 10:47:43, localpref 100, from 10.255.0.1
AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299776
2:10.255.0.2:100::100::00:00:00:00:02::10.0.0.2/304
*[BGP/170] 10:41:55, localpref 100, from 10.255.0.2
AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299808
2:10.255.0.2:100::100::00:11:22:33:44:55::10.0.0.250/304
*[BGP/170] 10:47:34, localpref 100, from 10.255.0.2
AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299808
2:10.255.0.2:100::100::00:11:22:33:44:55::10.0.0.252/304
*[BGP/170] 10:47:34, localpref 100, from 10.255.0.2
AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299808
2:10.255.0.3:100::100::00:00:00:00:03::10.0.0.3/304
*[EVPN/170] 10:59:05
Indirect
2:10.255.0.3:100::100::00:05:86:71:79:f0::10.0.0.253/304
*[EVPN/170] 11:00:23
Indirect
3:10.255.0.1:100::100::10.255.0.1/304
*[BGP/170] 10:47:43, localpref 100, from 10.255.0.1
AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299776
3:10.255.0.2:100::100::10.255.0.2/304
*[BGP/170] 10:47:34, localpref 100, from 10.255.0.2
AS path: I, validation-state: unverified
> to 198.51.100.6 via ge-0/0/0.0, Push 299808
3:10.255.0.3:100::100::10.255.0.3/304
*[EVPN/170] 10:59:40
Indirect

```

Meaning The remote type 1 autodiscovery route is received for the ESI attached to Router PE2, which is the other PE router connected to the multihomed CE device.

Verifying the Ethernet Segment Route

Purpose Verify that the local and advertised autodiscovery routes per Ethernet segment and the Ethernet segment routes are received.

Router PE1 Action

From operational mode, run the **show route table __default_evpn__.evpn.0** command.

```
user@PE1> show route table __default_evpn__.evpn.0
__default_evpn__.evpn.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1:10.255.0.1:0::112233445566778899::0/304
    * [EVPN/170] 3d 00:00:31
    Indirect
1:10.255.0.1:0::224466880022446688::0/304
    * [EVPN/170] 3d 00:00:31
    Indirect
4:10.255.0.1:0::112233445566778899:10.255.0.1/304
    * [EVPN/170] 3d 00:00:31
    Indirect
4:10.255.0.1:0::224466880022446688:10.255.0.1/304
    * [EVPN/170] 3d 00:00:31
    Indirect
4:10.255.0.2:0::112233445566778899:10.255.0.2/304
    * [BGP/170] 3d 00:00:20, localpref 100, from 10.255.0.2
    AS path: I, validation-state: unverified
    > to 198.51.100.2 via ge-0/0/0.0, Push 299808
4:10.255.0.2:0::224466880022446688:10.255.0.2/304
    * [BGP/170] 3d 00:00:20, localpref 100, from 10.255.0.2
    AS path: I, validation-state: unverified
    > to 198.51.100.2 via ge-0/0/0.0, Push 299808
```

Router PE2

From operational mode, run the **show route table __default_evpn__.evpn.0** command.

```
user@PE2> show route table __default_evpn__.evpn.0
__default_evpn__.evpn.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1:10.255.0.2:0::112233445566778899::0/304
    * [EVPN/170] 10:49:26
    Indirect
1:10.255.0.2:0::224466880022446688::0/304
    * [EVPN/170] 10:49:26
    Indirect
4:10.255.0.1:0::112233445566778899:10.255.0.1/304
    * [BGP/170] 10:49:26, localpref 100, from 10.255.0.1
    AS path: I, validation-state: unverified
    > to 198.51.100.4 via ge-0/0/0.0, Push 299776
4:10.255.0.1:0::224466880022446688:10.255.0.1/304
    * [BGP/170] 10:49:26, localpref 100, from 10.255.0.1
    AS path: I, validation-state: unverified
    > to 198.51.100.4 via ge-0/0/0.0, Push 299776
4:10.255.0.2:0::112233445566778899:10.255.0.2/304
    * [EVPN/170] 10:49:26
    Indirect
```

```

4:10.255.0.2:0::224466880022446688:10.255.0.2/304
*[EVPN/170] 10:49:26
Indirect

```

Meaning The output displays the local and remote type 1 (autodiscovery) and type 4 (Ethernet segment) routes:

- **1:10.255.0.1:0::112233445566778899:0/304**—Autodiscovery route per Ethernet segment for each local ESI attached to Router PE1 and Router PE2.
- **4:10.255.0.1:0::112233445566778899:10.255.0.1/304**—Ethernet segment route for each local ESI attached to Router PE1 and Router PE2.
- **4:10.255.0.2:0::112233445566778899:10.255.0.2/304**—Remote Ethernet segment route from Router PE2.

Verifying the DF Status

Purpose Confirm which PE router is the designated forwarder (DF).

Action From operational mode, run the **show evpn instance ALPHA esi esi designated-forwarder** command.

```

user@PE1> show evpn instance ALPHA esi 00:11:22:33:44:55:66:77:88:99
designated-forwarder
Instance: ALPHA
  Number of ethernet segments: 1
  ESI: 00:11:22:33:44:55:66:77:88:99
  Designated forwarder: 10.255.0.1

```

Meaning Router PE1 is the DF for the ALPHA routing instance.

Verifying the BDF Status

Purpose Confirm which PE router is the backup designated forwarder (BDF).

Action From operational mode, run the **show evpn instance ALPHA esi esi backup-forwarder** command.

```

user@PE1> show evpn instance ALPHA esi 00:11:22:33:44:55:66:77:88:99
backup-forwarder
Instance: ALPHA
  Number of ethernet segments: 1
  ESI: 00:11:22:33:44:55:66:77:88:99
  Backup forwarder: 10.255.0.2

```

Meaning Router PE2 is the BDF for the ALPHA routing instance.

Verifying Remote IRB MAC

Purpose Verify that the remote gateway MAC addresses are synchronized among all the PE routers.

Router PE1 Action

From operational mode, run the **show bridge evpn peer-gateway-mac** command.

```
user@PE1> show bridge evpn peer-gateway-mac
Routing instance : ALPHA
Bridging domain : ONE, VLAN : 100
Installed GW MAC addresses:
00:05:86:71:79:f0
```

Router PE2

From operational mode, run the **show bridge evpn peer-gateway-mac** command.

```
user@PE2> show bridge evpn peer-gateway-mac
Routing instance : ALPHA
Bridging domain : ONE, VLAN : 100
Installed GW MAC addresses:
00:05:86:71:79:f0
```

Router PE3

From operational mode, run the **show bridge evpn peer-gateway-mac** command.

```
user@PE2> show bridge evpn peer-gateway-mac
Routing instance : ALPHA
Bridging domain : ONE, VLAN : 100
Installed GW MAC addresses:
00:11:22:33:44:55
```

Meaning The remote gateway MAC addresses are synchronized:

- Router PE3 gateway MAC is installed in Routers PE1 and PE2 peer-gateway-mac table.
- Routers PE1 and PE2 gateway MAC addresses are installed in Router PE3 peer-gateway-mac table.

Verifying Remote IRB and Host IP

Purpose Verify that the remote IRB IP and the host IP are received.

Router PE1 Action

From operational mode, run the **show route table DELTA** command.

```
user@PE1> show route table DELTA
DELTA.inet.0: 16 destinations, 18 routes (16 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.0.0/24          *[Direct/0] 11:25:54
                    > via irb.0
                    [Direct/0] 11:25:54
                    > via irb.0
10.0.0.1/32          *[EVPN/7] 11:21:33
                    > via irb.0
10.0.0.2/32          *[EVPN/7] 11:20:06, metric2 1
                    > to 198.51.100.2 via ge-0/0/0.0, Push 300208, Push 299808(top)
```

```

10.0.0.3/32      *[EVPN/7] 11:25:54, metric2 1
                 > to 198.51.100.2 via ge-0/0/0.0, Push 299776, Push 299792(top)
10.0.0.4/32      *[EVPN/7] 11:24:47
                 > via irb.0
10.0.0.250/32    *[Local/0] 11:38:29
                 Local via irb.0
10.0.0.251/32    *[Local/0] 11:38:29
                 Local via irb.0
10.0.0.253/32    *[EVPN/7] 11:25:54, metric2 1
                 > to 198.51.100.2 via ge-0/0/0.0, Push 299776, Push 299792(top)
192.0.2.0/24     *[Direct/0] 11:25:55
                 > via irb.1
                 [Direct/0] 11:25:55
                 > via irb.1
192.0.2.1/24     *[EVPN/7] 11:21:20
                 > via irb.1
192.0.2.2/24     *[EVPN/7] 11:19:54, metric2 1
                 > to 198.51.100.2 via ge-0/0/0.0, Push 300240, Push 299808(top)
192.0.2.3/24     *[EVPN/7] 11:25:54, metric2 1
                 > to 198.51.100.2 via ge-0/0/0.0, Push 299808, Push 299792(top)
192.0.2.4/24     *[EVPN/7] 11:24:40
                 > via irb.1
192.0.2.10/24    *[Local/0] 11:38:29
                 Local via irb.1
192.0.2.15/24    *[Local/0] 11:38:29
                 Local via irb.1
192.0.2.13/24    *[EVPN/7] 11:25:54, metric2 1
                 > to 198.51.100.2 via ge-0/0/0.0, Push 299808, Push 299792(top)

```

Router PE2

From operational mode, run the **show route table DELTA** command.

```

user@PE2> show route table DELTA
DELTA.inet.0: 16 destinations, 18 routes (16 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.0.0/24      *[Direct/0] 11:30:02
                 > via irb.0
                 [Direct/0] 11:30:02
                 > via irb.0
10.0.0.1/32      *[EVPN/7] 11:25:50, metric2 1
                 > to 198.51.100.4 via ge-0/0/0.0, Push 300144, Push 299776(top)
10.0.0.2/32      *[EVPN/7] 11:24:23
                 > via irb.0
10.0.0.3/32      *[EVPN/7] 11:30:02, metric2 1
                 > to 198.51.100.4 via ge-0/0/0.0, Push 299776, Push 299792(top)
10.0.0.4/32      *[EVPN/7] 11:29:04, metric2 1
                 > to 198.51.100.4 via ge-0/0/0.0, Push 300144, Push 299776(top)
10.0.0.250/32    *[Local/0] 11:42:33
                 Local via irb.0
10.0.0.252/32    *[Local/0] 11:42:33
                 Local via irb.0
10.0.0.253/32    *[EVPN/7] 11:30:02, metric2 1
                 > to 198.51.100.4 via ge-0/0/0.0, Push 299776, Push 299792(top)
192.0.0.0/24     *[Direct/0] 11:30:02
                 > via irb.1
                 [Direct/0] 11:30:02
                 > via irb.1
192.0.2.1/24     *[EVPN/7] 11:25:37, metric2 1
                 > to 198.51.100.4 via ge-0/0/0.0, Push 300176, Push 299776(top)

```

```

192.0.2.2/24      *[EVPN/7] 11:24:11
                  > via irb.1
192.0.2.3/24      *[EVPN/7] 11:30:02, metric2 1
                  > to 198.51.100.4 via ge-0/0/0.0, Push 299808, Push 299792(top)
192.0.2.4/24      *[EVPN/7] 11:28:57, metric2 1
                  > to 198.51.100.4 via ge-0/0/0.0, Push 300176, Push 299776(top)
192.0.2.10/24     *[Local/0] 11:42:33
                  Local via irb.1
192.0.2.12/24     *[Local/0] 11:42:33
                  Local via irb.1
192.0.2.13/24     *[EVPN/7] 11:30:02, metric2 1
                  > to 198.51.100.4 via ge-0/0/0.0, Push 299808, Push 299792(top)

```

Router PE3

From operational mode, run the **show route table DELTA** command.

```

user@PE3> show route table DELTA
DELTA.inet.0: 16 destinations, 16 routes (16 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.0.0/24      *[Direct/0] 11:42:15
                  > via irb.0
10.0.0.1/32      *[EVPN/7] 11:25:56, metric2 1
                  > to 198.51.100.6 via ge-0/0/0.0, Push 300144, Push 299776(top)
10.0.0.2/32      *[EVPN/7] 11:24:29, metric2 1
                  > to 198.51.100.6 via ge-0/0/0.0, Push 300208, Push 299808(top)
10.0.0.3/32      *[EVPN/7] 11:41:39
                  > via irb.0
10.0.0.4/32      *[EVPN/7] 11:29:10, metric2 1
                  > to 198.51.100.6 via ge-0/0/0.0, Push 300144, Push 299776(top)
10.0.0.250/32    *[EVPN/7] 11:30:08, metric2 1
                  > to 198.51.100.6 via ge-0/0/0.0, Push 300208, Push 299808(top)
10.0.0.252/32    *[EVPN/7] 11:30:08, metric2 1
                  > to 198.51.100.6 via ge-0/0/0.0, Push 300208, Push 299808(top)
10.0.0.253/32    *[Local/0] 11:42:57
                  Local via irb.0
192.0.0.0/24     *[Direct/0] 11:42:15
                  > via irb.1
192.0.2.1/24     *[EVPN/7] 11:25:43, metric2 1
                  > to 198.51.100.6 via ge-0/0/0.0, Push 300176, Push 299776(top)
192.0.2.2/24     *[EVPN/7] 11:24:17, metric2 1
                  > to 198.51.100.6 via ge-0/0/0.0, Push 300240, Push 299808(top)
192.0.2.3/24     *[EVPN/7] 11:42:04
                  > via irb.1
192.0.2.4/24     *[EVPN/7] 11:29:03, metric2 1
                  > to 198.51.100.6 via ge-0/0/0.0, Push 300176, Push 299776(top)
192.0.2.10/24    *[EVPN/7] 11:30:08, metric2 1
                  > to 198.51.100.6 via ge-0/0/0.0, Push 300240, Push 299808(top)
192.0.2.12/24    *[EVPN/7] 11:30:08, metric2 1
                  > to 198.51.100.6 via ge-0/0/0.0, Push 300240, Push 299808(top)
192.0.2.13/24    *[Local/0] 11:42:57
                  Local via irb.1

```

Meaning The output displays the local and remote IRB interfaces. It also displays the local and remote hosts that are installed in the VRF table:

On Router PE1:

- **10.0.0.1/32**—Local host in the virtual switch routing instance.
- **10.0.0.2/32** and **10.0.0.3/32**—Remote host in the virtual switch routing instance.
- **10.0.0.250/32**—Local IRB in the virtual switch routing instance.
- **10.0.0.253/32**—Remote IRB in the virtual switch routing instance.

Verifying ARP Table

Purpose Verify the ARP table entries.

Router PE1 Action

From operational mode, run the **show evpn arp-table** command.

```
user@PE1> show evpn arp-table
INET          MAC          Logical      Routing      Bridging
address       address      interface    instance     domain
192.0.2.1     00:00:00:00:00:01  irb.1       BETA         __BETA__
192.0.2.4     00:00:00:00:00:04  irb.1       BETA         __BETA__
```

Router PE2

From operational mode, run the **show evpn arp-table** command.

```
user@PE2> show evpn arp-table
INET          MAC          Logical      Routing      Bridging
address       address      interface    instance     domain
192.0.2.2     00:00:00:00:00:02  irb.1       BETA         __BETA__
```

Router PE3

From operational mode, run the **show evpn arp-table** command.

```
user@PE3> show evpn arp-table
INET          MAC          Logical      Routing      Bridging
address       address      interface    instance     domain
192.0.2.3     00:00:00:00:00:03  irb.1       BETA         __BETA__
```

Meaning The EVPN instance and ARP are synchronized with the host MAC and IP address for local hosts.

Verifying Bridge ARP Table

Purpose Verify the bridge ARP table entries.

Router PE1 Action

From operational mode, run the **show bridge evpn arp-table** command.

```
user@PE3> show bridge evpn arp-table
INET          MAC          Logical      Routing      Bridging
address       address      interface    instance     domain
```

10.0.0.1	00:00:00:00:00:01	irb.0	ALPHA	ONE
10.0.0.4	00:00:00:00:00:04	irb.0	ALPHA	ONE

Router PE2

From operational mode, run the **show bridge evpn arp-table** command.

```
user@PE3> show bridge evpn arp-table
INET          MAC          Logical      Routing      Bridging
address       address       interface    instance     domain
10.0.0.2      00:00:00:00:00:02  irb.0        ALPHA        ONE
```

Router PE3

From operational mode, run the **show bridge evpn arp-table** command.

```
user@PE3> show bridge evpn arp-table
INET          MAC          Logical      Routing      Bridging
address       address       interface    instance     domain
10.0.0.3      00:00:00:00:00:03  irb.0        ALPHA        ONE
```

Meaning The virtual switch instance and ARP are synchronized with the local host MAC and IP address.

Verifying Bridge MAC Table

Purpose Verify the bridge MAC table entries.

Router PE1 Action

From operational mode, run the **show bridge mac-table** command.

```
user@PE1> show bridge mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
          SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : ALPHA
Bridging domain : ONE, VLAN : 100
MAC          MAC          Logical      NH      RTR
address      flags      interface    Index   ID
00:00:00:00:00:01  D          ge-0/0/2.0   1048583 1048583
00:00:00:00:00:02  DC                      1048574 1048574
00:00:00:00:00:03  DC                      1048574 1048574
00:00:00:00:00:04  D          ae0.0
```

Router PE2

From operational mode, run the **show bridge mac-table** command.

```
user@PE2> show bridge mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
          SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : ALPHA
Bridging domain : ONE, VLAN : 100
MAC          MAC          Logical      NH      RTR
address      flags      interface    Index   ID
00:00:00:00:00:01  DC                      1048577 1048577
```

```
00:00:00:00:00:02 D ge-0/0/2.0
00:00:00:00:00:03 DC 1048578 1048578
00:00:00:00:00:04 DC 1048577 1048577
```

Router PE3

From operational mode, run the **show bridge mac-table** command.

```
user@PE3> show bridge mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
          SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : ALPHA
Bridging domain : ONE, VLAN : 100
MAC address      MAC flags      Logical interface  NH Index  RTR ID
00:00:00:00:00:01 DC              1048575 1048575
00:00:00:00:00:02 DC              1048582 1048582
00:00:00:00:00:03 D ae0.0
00:00:00:00:00:04 DC              1048575 1048575
```

Meaning The virtual switch instance installed local and remote host MAC addresses in the bridge MAC table.

Related Documentation

- [EVPN Multihoming Overview on page 245](#)

CHAPTER 20

Configuring Integrated Bridging and Routing Using EVPNs

- [EVPN with IRB Solution Overview on page 298](#)
- [Configuring EVPN with IRB Solution on page 302](#)
- [Example: Configuring EVPN with IRB Solution on page 304](#)

EVPN with IRB Solution Overview

A Data Center Service Provider (DCSP) hosts the data center for its multiple customers onto a common physical network. To each customer (also called a tenant), the service looks like a full-fledged data center that can expand to 4094 VLANs and all private subnets. For disaster recovery, high availability, and optimization of resource utilization, it is common for the DCSP to span the data center to more than one site. In order to deploy the data center services, a DCSP faces the following main challenges:

- Extending Layer 2 domains across more than one data center site. This requires optimal intra-subnet traffic forwarding.
- Supporting optimal inter-subnet traffic forwarding and optimal routing in the event of virtual machine (VM) motion.
- Supporting multiple tenants with independent VLAN and subnet space.

Ethernet VPN (EVPN) is targeted to handle all of the above mentioned challenges, wherein:

- The basic EVPN functionality enables optimal intra-subnet traffic forwarding
- Implementing the integrated routing and bridging (IRB) solution in an EVPN deployment enables optimal inter-subnet traffic forwarding
- Configuring EVPN with virtual switch support enables multiple tenants with independent VLAN and subnet space

The following sections describe the integrated routing and bridging (IRB) solution for EVPNs:

- [Need for an EVPN IRB Solution on page 298](#)
- [Implementing the EVPN IRB Solution on page 299](#)
- [Benefits of Implementing the EVPN IRB Solution on page 301](#)

Need for an EVPN IRB Solution

EVPN is a technology used to provide Layer 2 extension and interconnection across an IP/MPLS core network to different physical sites belonging to a single Layer 2 domain. In a data center environment with EVPN, there is a need for both Layer 2 (intra-subnet traffic) and Layer 3 (inter-subnet traffic) forwarding and potentially interoperability with tenant Layer 3 VPNs.

With only a Layer 2 solution, there is no optimum forwarding of inter-subnet traffic, even when the traffic is local, for instance, when both the subnets are on the same server.

With only a Layer 3 solution, the following issues for intra-subnet traffic can arise:

- MAC address aliasing issue where duplicate MAC addresses are not detected.
- TTL issue for applications that use TTL 1 to confine traffic within a subnet.

- IPv6 link-local addressing and duplicate address detection that relies on Layer 2 connectivity.
- Layer 3 forwarding does not support the forwarding semantics of a subnet broadcast.
- Support of non-IP applications that require Layer 2 forwarding.

Because of the above mentioned shortcomings of a pure Layer 2 and Layer 3 solution, there is a need for a solution incorporating optimal forwarding of both Layer 2 and Layer 3 traffic in the data center environment when faced with operational considerations such as Layer 3 VPN interoperability and virtual machine (VM) mobility.

An EVPN-based integrated routing and bridging (IRB) solution provides optimum unicast and multicast forwarding for both intra-subnets and inter-subnets within and across data centers.

The EVPN IRB feature is useful for service providers operating in an IP/MPLS network that provides both Layer 2 VPN or VPLS services and Layer 3 VPN services who want to extend their service to provide cloud computation and storage services to their existing customers.

Implementing the EVPN IRB Solution

An EVPN IRB solution provides the following:

- Optimal forwarding for intra-subnet (Layer 2) traffic.
- Optimal forwarding for inter-subnet (Layer 3) traffic.
- Support for ingress replication for multicast traffic.
- Support for network-based as well as host-based overlay models.
- Support for consistent policy-based forwarding for both Layer 2 and Layer 3 traffic.

Junos OS supports several models of EVPN configuration to satisfy the individual needs of EVPN and data center cloud services customers. To provide flexibility and scalability, multiple bridge domains can be defined within a particular EVPN instance. Likewise, one or more EVPN instances can be associated with a single Layer 3 VPN virtual routing and forwarding (VRF). In general, each data center tenant is assigned a unique Layer 3 VPN VRF, while a tenant could comprise one or more EVPN instances and one or more bridge domains per EVPN instance. To support this model, each configured bridge domain (including the default bridge domain for an EVPN instance) requires an IRB interface to perform the Layer 2 and Layer 3 functions. Each bridge domain or IRB interface maps to a unique IP subnet in the VRF.



NOTE: You can associate an IRB interface with the master instance inet.0 table instead of a VRF in an EVPN IRB solution.

There are two major functions that are supported for IRB in EVPN.

- Host MAC-IP synchronization

This includes:

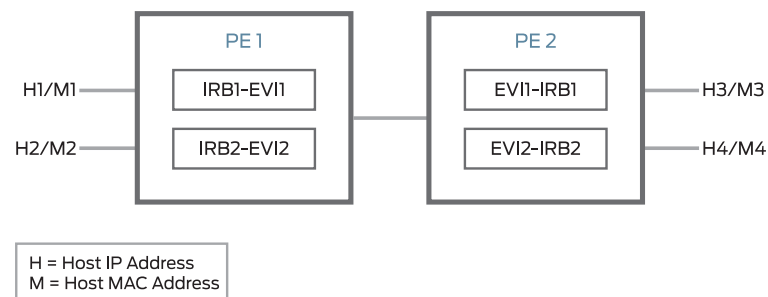
- Advertising the IP address along with the MAC advertisement route in EVPN. This is done by using the IP field in the EVPN MAC advertisement route.
- The receiving PE router installs MAC into the EVPN instance (EVI) table and installs IP into the associated VRF.
- Gateway MAC-IP synchronization

This includes:

- Advertising all local IRB MAC and IP addresses in an EVPN. This is achieved by including the default gateway extended community in the EVPN MAC advertisement route.
- The receiving PE creates a forwarding state to route packets destined for the gateway MAC, and a proxy ARP is done for the gateway IP with the MAC advertised in the route.

Figure 23 on page 300 illustrates the inter-subnet traffic forwarding between two provider edge (PE) devices – PE1 and PE2. The IRB1 and IRB2 interfaces on each PE device belong to a different subnet, but they share a common VRF.

Figure 23: Inter-Subnet Traffic Forwarding



The inter-subnet traffic forwarding is performed as follows:

1. PE2 advertises H3-M3 and H4-M4 binding to PE1. Similarly PE1 advertises H1-M1 and H2-M2 binding to PE2.
2. PE1 and PE2 install the MAC address in the corresponding EVI MAC table, whereas the IP routes are installed in the shared VRF.
3. The advertising PE device is set as the next hop for the IP routes.
4. If H1 sends packets to H4, the packets are sent to IRB1 on PE1.
5. IP lookup for H4 happens in the shared VRF on PE1. Because the next hop for the H4 IP is PE2 (the advertising PE), an IP unicast packet is sent to PE2.
6. PE1 rewrites the MAC header based on the information in the VRF route, and PE2 performs a MAC lookup to forward the packet to H4.

Benefits of Implementing the EVPN IRB Solution

The main goal of the EVPN IRB solution is to provide optimal Layer 2 and Layer 3 forwarding. The solution is required to efficiently handle inter-subnet forwarding as well as virtual machine (VM) mobility. VM mobility refers to the ability of a VM to migrate from one server to another within the same or a different data center while retaining its existing MAC and IP address. Providing optimal forwarding for inter-subnet traffic and effective VM mobility involves solving two problems – the default gateway problem and the triangular routing problem.

- [Gateway MAC and IP Synchronization on page 301](#)
- [Layer 3 VPN Interworking on page 301](#)

Gateway MAC and IP Synchronization

In an EVPN IRB deployment, the IP default gateway for a VM is the IP address configured on the IRB interface of the provider edge (PE) router corresponding to the bridge domain or VLAN of which the VM is a member. The default gateway problem arises because a VM does not flush its ARP table when relocating from one server to another and continues sending packets with the destination MAC address set to that of the original gateway. If the old and new servers are not part of the same Layer 2 domain (the new Layer 2 domain could be within the current data center or a new data center), the gateway previously identified is no longer the optimal or local gateway. The new gateway needs to identify packets containing the MAC addresses of other gateways on remote PE routers and forward the traffic as if the packets were destined to the local gateway itself. At the minimum, this functionality requires each PE router to advertise its gateway or IRB MAC and IP addresses to all other PE routers in the network. The gateway address exchange can be accomplished using the standard MAC route advertisement message (including the IP address parameter) and tagging that route with the default gateway extended community so that the remote PE routers can distinguish the gateway MAC advertisement routes from normal MAC advertisement routes.

Layer 3 VPN Interworking

The inter-data center aspect of the EVPN IRB solution involves routing between VMs that are present in different data centers or routing between a host site completely outside of the data center environment and a VM within a data center. This solution relies on the ability of EVPN MAC route advertisements to carry both MAC address and IP address information. The local MAC learning functionality of the PE router is extended to also capture IP address information associated with MAC addresses learned locally. That IP-MAC address mapping information is then distributed to each PE router through normal EVPN procedures. When a PE router receives such MAC and IP information, it installs the MAC route in the EVPN instance as well as a host route for the associated IP address in the Layer 3 VPN VRF corresponding to that EVPN instance. When a VM moves from one data center to another, normal EVPN procedures result in the MAC and IP address being advertised from the new PE router which the VM resides behind. The host route installed in the VRF associated with an EVPN solicits Layer 3 traffic destined to that VM to the new PE router and avoids triangular routing between the source, the former PE router the VM resided behind, and the new PE router.

BGP scalability is a potential concern with the inter-data center triangular routing avoidance solution because of the potential for injection of many host routes into Layer 3 VPN. With the method previously described, in the worst case there is an IP host route for each MAC address learned through the local EVPN MAC learning procedures or through a MAC advertisement message received from a remote PE router. BGP route target filtering can be used to limit distribution of such routes.

The following functional elements are required to implement the inter-data center triangular routing avoidance using Layer 3 inter-subnet forwarding procedures:

1. The source host sends an IP packet using its own source MAC and IP address with the destination MAC of the IRB interface of the local PE router and the IP address of the destination host.
2. When the IRB interface receives the frame with its MAC as the destination, it performs a Layer 3 lookup in the VRF associated with the EVPN instance to determine where to route the packet.
3. In the VRF, the PE router finds the Layer 3 route derived from a MAC plus an IP EVPN route received from the remote PE router earlier. The destination MAC address is then changed to the destination MAC address corresponding to the destination IP.
4. The packet is then forwarded to the remote PE router serving the destination host using MPLS, using the label corresponding to the EVPN instance of which the destination host is a member.
5. The egress PE router receiving the packet performs a Layer 2 lookup for the destination host's MAC and sends the packet to the destination host on the attached subnet via the egress PE router's IRB interface.
6. Because the ingress PE router is performing Layer 3 routing, the IP TTL is decremented.

**Related
Documentation**

- [Example: Configuring EVPN with IRB Solution on page 309](#)

Configuring EVPN with IRB Solution

You can configure an Ethernet VPN (EVPN) with IRB solution to enable Layer 2 switching and Layer 3 routing operations within a single node, thus avoiding extra hops for inter-subnet traffic. The EVPN IRB solution eliminates the default gateway problem using the gateway MAC and IP synchronization, and avoids the triangular routing problem with Layer 3 interworking by creating IP host routes for virtual machines (VMs) in the tenant virtual routing and forwarding (VRF) routing instances.

Before you begin:

1. Configure the router interfaces.
2. Configure the router ID and autonomous system number for the device.
3. Enable chained composite next hop for EVPN.
4. Configure OSPF or any other IGP protocol.

5. Configure a BGP internal group.
6. Include the EVPN signaling network layer reachability information (NLRI) to the internal BGP group.
7. Configure RSVP or LDP.
8. Configure MPLS.
9. Create a label-switched path between the provider edge (PE) devices.

To configure the PE device:

1. Configure the EVPN routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance instance-type evpn
```

2. Set the VLAN identifier for the bridging domain in the EVPN routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance vlan-id VLAN-ID
```

3. Configure the interface name for the EVPN routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance interface CE-facing-interface
```

4. Configure the IRB interface as the routing interface for the EVPN routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance routing-interface irb.0
```

5. Configure the route distinguisher for the EVPN routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance route-distinguisher route-distinguisher-value
```

6. Configure the VPN routing and forwarding (VRF) target community for the EVPN routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance vrf-target vrf-target-value
```

7. Assign the interface name that connects the PE device site to the VPN.

```
[edit routing-instances]
user@PE1# set evpn-instance protocols evpn interface CE-facing-interface
```

8. Configure the VRF routing instance.

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

9. Configure the IRB interface as the routing interface for the VRF routing instance.

```
[edit routing-instances]
user@PE1# set vrf-instance interface irb.0
```

10. Configure the route distinguisher for the VRF routing instance.

```
[edit routing-instances]
user@PE1# set vrf-instance route-distinguisher route-distinguisher-value
```

11. Configure the VRF label for the VRF routing instance.

```
[edit routing-instances]
user@PE1# set vrf-instance vrf-table-label
```

12. Verify and commit the configuration.

For example:

```
[edit routing-instances]
user@PE1# set evpna instance-type evpn
user@PE1# set evpna vlan-id 10
user@PE1# set evpna interface ge-1/1/8.0
user@PE1# set evpna routing-interface irb.0
user@PE1# set evpna route-distinguisher 192.0.2.1:100
user@PE1# set evpna vrf-target target:100:100
user@PE1# set evpna protocols evpn interface ge-1/1/8.0
user@PE1# set vrf instance-type vrf
user@PE1# set vrf interface irb.0
user@PE1# set vrf route-distinguisher 192.0.2.1:300
user@PE1# set vrf vrf-target target:100:300
user@PE1# set vrf vrf-table-label

[edit]
user@PE1# commit
commit complete
```

Related Documentation

- [Example: Configuring EVPN with IRB Solution on page 304](#)

Example: Configuring EVPN with IRB Solution

- [EVPN with IRB Solution Overview on page 305](#)
- [Example: Configuring EVPN with IRB Solution on page 309](#)

EVPN with IRB Solution Overview

A Data Center Service Provider (DCSP) hosts the data center for its multiple customers onto a common physical network. To each customer (also called a tenant), the service looks like a full-fledged data center that can expand to 4094 VLANs and all private subnets. For disaster recovery, high availability, and optimization of resource utilization, it is common for the DCSP to span the data center to more than one site. In order to deploy the data center services, a DCSP faces the following main challenges:

- Extending Layer 2 domains across more than one data center site. This requires optimal intra-subnet traffic forwarding.
- Supporting optimal inter-subnet traffic forwarding and optimal routing in the event of virtual machine (VM) motion.
- Supporting multiple tenants with independent VLAN and subnet space.

Ethernet VPN (EVPN) is targeted to handle all of the above mentioned challenges, wherein:

- The basic EVPN functionality enables optimal intra-subnet traffic forwarding
- Implementing the integrated routing and bridging (IRB) solution in an EVPN deployment enables optimal inter-subnet traffic forwarding
- Configuring EVPN with virtual switch support enables multiple tenants with independent VLAN and subnet space

The following sections describe the integrated routing and bridging (IRB) solution for EVPNs:

- [Need for an EVPN IRB Solution on page 305](#)
- [Implementing the EVPN IRB Solution on page 306](#)
- [Benefits of Implementing the EVPN IRB Solution on page 308](#)

Need for an EVPN IRB Solution

EVPN is a technology used to provide Layer 2 extension and interconnection across an IP/MPLS core network to different physical sites belonging to a single Layer 2 domain. In a data center environment with EVPN, there is a need for both Layer 2 (intra-subnet traffic) and Layer 3 (inter-subnet traffic) forwarding and potentially interoperability with tenant Layer 3 VPNs.

With only a Layer 2 solution, there is no optimum forwarding of inter-subnet traffic, even when the traffic is local, for instance, when both the subnets are on the same server.

With only a Layer 3 solution, the following issues for intra-subnet traffic can arise:

- MAC address aliasing issue where duplicate MAC addresses are not detected.
- TTL issue for applications that use TTL 1 to confine traffic within a subnet.
- IPv6 link-local addressing and duplicate address detection that relies on Layer 2 connectivity.

- Layer 3 forwarding does not support the forwarding semantics of a subnet broadcast.
- Support of non-IP applications that require Layer 2 forwarding.

Because of the above mentioned shortcomings of a pure Layer 2 and Layer 3 solution, there is a need for a solution incorporating optimal forwarding of both Layer 2 and Layer 3 traffic in the data center environment when faced with operational considerations such as Layer 3 VPN interoperability and virtual machine (VM) mobility.

An EVPN-based integrated routing and bridging (IRB) solution provides optimum unicast and multicast forwarding for both intra-subnets and inter-subnets within and across data centers.

The EVPN IRB feature is useful for service providers operating in an IP/MPLS network that provides both Layer 2 VPN or VPLS services and Layer 3 VPN services who want to extend their service to provide cloud computation and storage services to their existing customers.

Implementing the EVPN IRB Solution

An EVPN IRB solution provides the following:

- Optimal forwarding for intra-subnet (Layer 2) traffic.
- Optimal forwarding for inter-subnet (Layer 3) traffic.
- Support for ingress replication for multicast traffic.
- Support for network-based as well as host-based overlay models.
- Support for consistent policy-based forwarding for both Layer 2 and Layer 3 traffic.

Junos OS supports several models of EVPN configuration to satisfy the individual needs of EVPN and data center cloud services customers. To provide flexibility and scalability, multiple bridge domains can be defined within a particular EVPN instance. Likewise, one or more EVPN instances can be associated with a single Layer 3 VPN virtual routing and forwarding (VRF). In general, each data center tenant is assigned a unique Layer 3 VPN VRF, while a tenant could comprise one or more EVPN instances and one or more bridge domains per EVPN instance. To support this model, each configured bridge domain (including the default bridge domain for an EVPN instance) requires an IRB interface to perform the Layer 2 and Layer 3 functions. Each bridge domain or IRB interface maps to a unique IP subnet in the VRF.



NOTE: You can associate an IRB interface with the master instance inet.0 table instead of a VRF in an EVPN IRB solution.

There are two major functions that are supported for IRB in EVPN.

- Host MAC-IP synchronization

This includes:

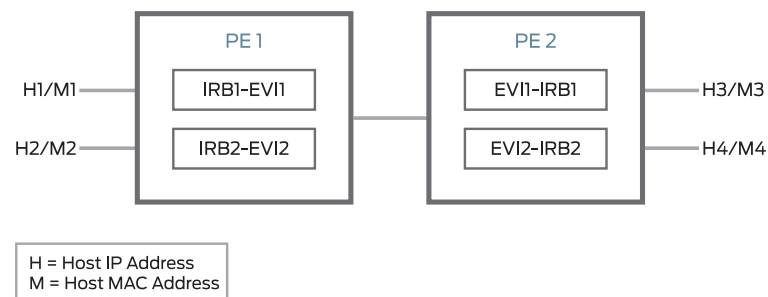
- Advertising the IP address along with the MAC advertisement route in EVPN. This is done by using the IP field in the EVPN MAC advertisement route.
- The receiving PE router installs MAC into the EVPN instance (EVI) table and installs IP into the associated VRF.
- Gateway MAC-IP synchronization

This includes:

- Advertising all local IRB MAC and IP addresses in an EVPN. This is achieved by including the default gateway extended community in the EVPN MAC advertisement route.
- The receiving PE creates a forwarding state to route packets destined for the gateway MAC, and a proxy ARP is done for the gateway IP with the MAC advertised in the route.

Figure 23 on page 300 illustrates the inter-subnet traffic forwarding between two provider edge (PE) devices – PE1 and PE2. The IRB1 and IRB2 interfaces on each PE device belong to a different subnet, but they share a common VRF.

Figure 24: Inter-Subnet Traffic Forwarding



The inter-subnet traffic forwarding is performed as follows:

1. PE2 advertises H3-M3 and H4-M4 binding to PE1. Similarly PE1 advertises H1-M1 and H2-M2 binding to PE2.
2. PE1 and PE2 install the MAC address in the corresponding EVI MAC table, whereas the IP routes are installed in the shared VRF.
3. The advertising PE device is set as the next hop for the IP routes.
4. If H1 sends packets to H4, the packets are sent to IRB1 on PE1.
5. IP lookup for H4 happens in the shared VRF on PE1. Because the next hop for the H4 IP is PE2 (the advertising PE), an IP unicast packet is sent to PE2.
6. PE1 rewrites the MAC header based on the information in the VRF route, and PE2 performs a MAC lookup to forward the packet to H4.

Benefits of Implementing the EVPN IRB Solution

The main goal of the EVPN IRB solution is to provide optimal Layer 2 and Layer 3 forwarding. The solution is required to efficiently handle inter-subnet forwarding as well as virtual machine (VM) mobility. VM mobility refers to the ability of a VM to migrate from one server to another within the same or a different data center while retaining its existing MAC and IP address. Providing optimal forwarding for inter-subnet traffic and effective VM mobility involves solving two problems – the default gateway problem and the triangular routing problem.

- [Gateway MAC and IP Synchronization on page 308](#)
- [Layer 3 VPN Interworking on page 308](#)

Gateway MAC and IP Synchronization

In an EVPN IRB deployment, the IP default gateway for a VM is the IP address configured on the IRB interface of the provider edge (PE) router corresponding to the bridge domain or VLAN of which the VM is a member. The default gateway problem arises because a VM does not flush its ARP table when relocating from one server to another and continues sending packets with the destination MAC address set to that of the original gateway. If the old and new servers are not part of the same Layer 2 domain (the new Layer 2 domain could be within the current data center or a new data center), the gateway previously identified is no longer the optimal or local gateway. The new gateway needs to identify packets containing the MAC addresses of other gateways on remote PE routers and forward the traffic as if the packets were destined to the local gateway itself. At the minimum, this functionality requires each PE router to advertise its gateway or IRB MAC and IP addresses to all other PE routers in the network. The gateway address exchange can be accomplished using the standard MAC route advertisement message (including the IP address parameter) and tagging that route with the default gateway extended community so that the remote PE routers can distinguish the gateway MAC advertisement routes from normal MAC advertisement routes.

Layer 3 VPN Interworking

The inter-data center aspect of the EVPN IRB solution involves routing between VMs that are present in different data centers or routing between a host site completely outside of the data center environment and a VM within a data center. This solution relies on the ability of EVPN MAC route advertisements to carry both MAC address and IP address information. The local MAC learning functionality of the PE router is extended to also capture IP address information associated with MAC addresses learned locally. That IP-MAC address mapping information is then distributed to each PE router through normal EVPN procedures. When a PE router receives such MAC and IP information, it installs the MAC route in the EVPN instance as well as a host route for the associated IP address in the Layer 3 VPN VRF corresponding to that EVPN instance. When a VM moves from one data center to another, normal EVPN procedures result in the MAC and IP address being advertised from the new PE router which the VM resides behind. The host route installed in the VRF associated with an EVPN solicits Layer 3 traffic destined to that VM to the new PE router and avoids triangular routing between the source, the former PE router the VM resided behind, and the new PE router.

BGP scalability is a potential concern with the inter-data center triangular routing avoidance solution because of the potential for injection of many host routes into Layer 3 VPN. With the method previously described, in the worst case there is an IP host route for each MAC address learned through the local EVPN MAC learning procedures or through a MAC advertisement message received from a remote PE router. BGP route target filtering can be used to limit distribution of such routes.

The following functional elements are required to implement the inter-data center triangular routing avoidance using Layer 3 inter-subnet forwarding procedures:

1. The source host sends an IP packet using its own source MAC and IP address with the destination MAC of the IRB interface of the local PE router and the IP address of the destination host.
2. When the IRB interface receives the frame with its MAC as the destination, it performs a Layer 3 lookup in the VRF associated with the EVPN instance to determine where to route the packet.
3. In the VRF, the PE router finds the Layer 3 route derived from a MAC plus an IP EVPN route received from the remote PE router earlier. The destination MAC address is then changed to the destination MAC address corresponding to the destination IP.
4. The packet is then forwarded to the remote PE router serving the destination host using MPLS, using the label corresponding to the EVPN instance of which the destination host is a member.
5. The egress PE router receiving the packet performs a Layer 2 lookup for the destination host's MAC and sends the packet to the destination host on the attached subnet via the egress PE router's IRB interface.
6. Because the ingress PE router is performing Layer 3 routing, the IP TTL is decremented.

Example: Configuring EVPN with IRB Solution

This example shows how to configure an integrated routing and bridging (IRB) solution in an Ethernet VPN (EVPN) deployment.

- [Requirements on page 309](#)
- [Overview on page 310](#)
- [Configuration on page 310](#)
- [Verification on page 316](#)

Requirements

This example uses the following hardware and software components:

- Two MX Series 3D Universal Edge Routers containing MPC FPCs configured as PE routers.
- Two customer edge (CE) routers, each connected to the PE routers.
- Junos OS Release 14.1 or later running on all the PE routers.

Before you begin:

1. Configure the router interfaces.
2. Configure OSPF or any other IGP protocol.
3. Configure BGP.
4. Configure RSVP or LDP.
5. Configure MPLS.

Overview

In an EVPN solution, multiple bridge domains can be defined within a particular EVPN instance, and one or more EVPN instances can be associated with a single Layer 3 VPN VRF. In general, each data center tenant is assigned a unique Layer 3 VPN virtual route forwarding (VRF), although the tenant can be comprised of one or more EVPN instances or bridge domains per EVPN instance.

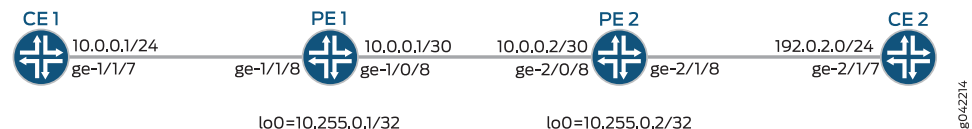
To support this flexibility and scalability factor, the EVPN solution provides support for the IRB interfaces on MX Series routers containing MPC FPCs to facilitate optimal Layer 2 and Layer 3 forwarding along with virtual machine mobility. The IRB interfaces are configured on each configured bridge domain including the default bridge domain for an EVPN instance.

IRB is the ability to do Layer 2 switching and Layer 3 routing within a single node, thus avoiding extra hops for inter-subnet traffic. The EVPN IRB solution eliminates the default gateway problem using the gateway MAC and IP synchronization, and avoids the triangular routing problem with Layer 3 interworking by creating IP host routes for virtual machines (VMs) in the tenant VRFs.

Topology

Figure 25 on page 310 illustrates a simple EVPN topology with IRB solution. Routers PE1 and PE2 are the provider edge routers that connect to two customer edge (CE) routers each – CE1 and CE2.

Figure 25: EVPN with IRB Solution



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.

```
CE1 set interfaces ge-1/1/7 vlan-tagging
    set interfaces ge-1/1/7 unit 0 vlan-id 10
    set interfaces ge-1/1/7 unit 0 family inet address 10.0.0.1/24
    set routing-options static route 192.0.2.0/24 next-hop 10.0.0.251
```

```

PE1  set interfaces ge-1/0/8 unit 0 family inet address 10.0.0.1/30
      set interfaces ge-1/0/8 unit 0 family mpls
      set interfaces ge-1/1/8 flexible-vlan-tagging
      set interfaces ge-1/1/8 encapsulation flexible-ethernet-services
      set interfaces ge-1/1/8 unit 0 encapsulation vlan-bridge
      set interfaces ge-1/1/8 unit 0 vlan-id 10
      set interfaces irb unit 0 family inet address 10.0.0.251/24
      set interfaces lo0 unit 0 family inet address 10.255.0.1/32
      set routing-options router-id 198.51.100.0
      set routing-options autonomous-system 100
      set routing-options forwarding-table chained-composite-next-hop ingress evpn
      set protocols rsvp interface all
      set protocols rsvp interface fxp0.0 disable
      set protocols mpls label-switched-path PE1-to-PE2 from 10.255.0.1
      set protocols mpls label-switched-path PE1-to-PE2 to 10.255.0.2
      set protocols mpls interface all
      set protocols mpls interface fxp0.0 disable
      set protocols bgp group ibgp type internal
      set protocols bgp group ibgp local-address 10.255.0.1
      set protocols bgp group ibgp family evpn signaling
      set protocols bgp group ibgp neighbor 10.255.0.2
      set protocols ospf area 0.0.0.0 interface all
      set protocols ospf area 0.0.0.0 interface fxp0.0 disable
      set routing-instances evpna instance-type evpn
      set routing-instances evpna vlan-id 10
      set routing-instances evpna interface ge-1/1/8.0
      set routing-instances evpna routing-interface irb.0
      set routing-instances evpna route-distinguisher 198.51.100.0:100
      set routing-instances evpna vrf-target target:100:100
      set routing-instances evpna protocols evpn interface ge-1/1/8.0
      set routing-instances vrf instance-type vrf
      set routing-instances vrf interface irb.0
      set routing-instances vrf route-distinguisher 198.51.100.0:300
      set routing-instances vrf vrf-target target:100:300
      set routing-instances vrf vrf-table-label

PE2  set interfaces ge-2/0/8 unit 0 family inet address 10.0.0.2/30
      set interfaces ge-2/0/8 unit 0 family mpls
      set interfaces ge-2/1/8 flexible-vlan-tagging
      set interfaces ge-2/1/8 encapsulation flexible-ethernet-services
      set interfaces ge-2/1/8 unit 0 encapsulation vlan-bridge
      set interfaces ge-2/1/8 unit 0 vlan-id 20
      set interfaces irb unit 0 family inet address 192.0.2.1/24
      set interfaces lo0 unit 0 family inet address 10.255.0.2/32
      set routing-options router-id 192.0.2.2
      set routing-options autonomous-system 100
      set routing-options forwarding-table chained-composite-next-hop ingress evpn
      set protocols rsvp interface all
      set protocols rsvp interface fxp0.0 disable
      set protocols mpls label-switched-path PE2-to-PE1 from 10.255.0.2
      set protocols mpls label-switched-path PE2-to-PE1 to 198.51.100.0
      set protocols mpls interface all
      set protocols mpls interface fxp0.0 disable
      set protocols bgp group ibgp type internal
      set protocols bgp group ibgp local-address 198.51.100.2

```

```

set protocols bgp group ibgp family evpn signaling
set protocols bgp group ibgp neighbor 198.51.100.1
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set routing-instances evpna instance-type evpn
set routing-instances evpna vlan-id 20
set routing-instances evpna interface ge-2/1/8.0
set routing-instances evpna routing-interface irb.0
set routing-instances evpna route-distinguisher 192.0.2.2:100
set routing-instances evpna vrf-target target:200:100
set routing-instances evpna protocols evpn interface ge-2/1/8.0
set routing-instances vrf instance-type vrf
set routing-instances vrf interface irb.0
set routing-instances vrf route-distinguisher 192.0.2.2:300
set routing-instances vrf vrf-target target:200:300
set routing-instances vrf vrf-table-label

```

```

CE2 set interfaces ge-2/1/7 unit 0 vlan-id 20
set interfaces ge-2/1/7 unit 0 family inet address 192.0.2.0/24
set routing-options static route 10.0.0.0/24 next-hop 192.0.2.5

```

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 Router PE1:



NOTE: Repeat this procedure for Router PE2, after modifying the appropriate interface names, addresses, and other parameters.

1. Configure Router PE1 interfaces.

[edit interfaces]

```

user@PE1# set ge-1/0/8 unit 0 family inet address 10.0.0.1/30
user@PE1# set ge-1/0/8 unit 0 family mpls

```

```

user@PE1# set ge-1/1/8 flexible-vlan-tagging
user@PE1# set ge-1/1/8 encapsulation flexible-ethernet-services
user@PE1# set ge-1/1/8 unit 0 encapsulation vlan-bridge
user@PE1# set ge-1/1/8 unit 0 vlan-id 10

```

```

user@PE1# set irb unit 0 family inet address 10.0.0.251/24

```

```

user@PE1# set lo0 unit 0 family inet address 10.255.0.1/32

```

2. Set the router ID and autonomous system number for Router PE1.

[edit routing-options]

```

user@PE1# set router-id 10.255.0.1
user@PE1# set autonomous-system 100

```

3. Configure the chained composite next hop for EVPN.

- ```
[edit routing-options]
user@PE1# set forwarding-table chained-composite-next-hop ingress evpn
```
4. Enable RSVP on all the interfaces of Router PE1, excluding the management interface.
 

```
[edit protocols]
user@PE1# set rsvp interface all
user@PE1# set rsvp interface fxp0.0 disable
```
  5. Create label-switched path for Router PE1 to reach Router PE2.
 

```
[edit protocols]
user@PE1# set mpls label-switched-path PE1-to-PE2 from 10.255.0.1
user@PE1# set mpls label-switched-path PE1-to-PE2 to 10.255.0.2
```
  6. Enable MPLS on all the interfaces of Router PE1, excluding the management interface.
 

```
[edit protocols]
user@PE1# set mpls interface all
user@PE1# set mpls mpls interface fxp0.0 disable
```
  7. Configure the BGP group for Router PE1.
 

```
[edit protocols]
user@PE1# set bgp group ibgp type internal
```
  8. Assign local and neighbor addresses to the ibgp BGP group for Router PE1 to peer with Router PE2.
 

```
[edit protocols]
user@PE1# set bgp group ibgp local-address 10.255.0.1
user@PE1# set bgp group ibgp neighbor 10.255.0.2
```
  9. Include the EVPN signaling Network Layer Reachability Information (NLRI) to the ibgp BGP group.
 

```
[edit protocols]
user@PE1# set bgp group ibgp family evpn signaling
```
  10. Configure OSPF on all the interfaces of Router PE1, excluding the management interface.
 

```
[edit protocols]
user@PE1# set ospf area 0.0.0.0 interface all
user@PE1# set ospf area 0.0.0.0 interface fxp0.0 disable
```
  11. Configure the EVPN routing instance.
 

```
[edit routing-instances]
user@PE1# set evpna instance-type evpn
```
  12. Set the VLAN identifier for the bridging domain in the evpna routing instance.
 

```
[edit routing-instances]
user@PE1# set evpna vlan-id 10
```
  13. Configure the interface name for the evpna routing instance.
 

```
[edit routing-instances]
user@PE1# set evpna interface ge-1/1/8.0
```

14. Configure the IRB interface as the routing interface for the evpna routing instance.

```
[edit routing-instances]
user@PE1# set evpna routing-interface irb.0
```

15. Configure the route distinguisher for the evpna routing instance.

```
[edit routing-instances]
user@PE1# set evpna route-distinguisher 10.255.0.1:100
```

16. Configure the VPN routing and forwarding (VRF) target community for the evpna routing instance.

```
[edit routing-instances]
user@PE1# set evpna vrf-target target:100:100
```

17. Assign the interface name that connects the PE1 site to the VPN.

```
[edit routing-instances]
user@PE1# set evpna protocols evpn interface ge-1/1/8.0
```

18. Configure the VRF routing instance.

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

19. Configure the IRB interface as the routing interface for the vrf routing instance.

```
[edit routing-instances]
user@PE1# set vrf interface irb.0
```

20. Configure the route distinguisher for the vrf routing instance.

```
[edit routing-instances]
user@PE1# set vrf route-distinguisher 10.255.0.1:300
```

21. Configure the VRF label for the vrf routing instance.

```
[edit routing-instances]
user@PE1# set vrf vrf-table-label
```

### **Results**

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

```
user@PE1# show interfaces
ge-1/0/8 {
 unit 0 {
 family inet {
 address 10.0.0.1/30;
 }
 family mpls;
 }
}
ge-1/1/8 {
 flexible-vlan-tagging;
 encapsulation flexible-ethernet-services;
 unit 0 {
```

```
 encapsulation vlan-bridge;
 vlan-id 10;
 }
}
irb {
 unit 0 {
 family inet {
 address 10.0.0.251/24;
 }
 }
}
lo0 {
 unit 0 {
 family inet {
 address 10.255.0.1/32 {
 }
 }
 }
}

user@PE1# show routing-options
router-id 10.255.0.1;
autonomous-system 100;
forwarding-table {
 chained-composite-next-hop {
 ingress {
 evpn;
 }
 }
}

user@PE1# show protocols
rsvp {
 interface all;
 interface fxp0.0 {
 disable;
 }
}
mpls {
 label-switched-path PE1-to-PE2 {
 from 10.255.0.1;
 to 10.255.0.2;
 }
 interface all;
 interface fxp0.0 {
 disable;
 }
}
bgp {
 group ibgp {
 type internal;
 local-address 10.255.0.1;
 family evpn {
 signaling;
 }
 neighbor 10.255.0.2;
 }
}
```

```
}
ospf {
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}

user@PE1# show routing-instances
evpna {
 instance-type evpn;
 vlan-id 10;
 interface ge-1/1/8.0;
 routing-interface irb.0;
 route-distinguisher 10.255.0.1:100;
 vrf-target target:100:100;
 protocols {
 evpn {
 interface ge-1/1/8.0;
 }
 }
}
vrf {
 instance-type vrf;
 interface irb.0;
 route-distinguisher 10.255.0.1:300;
 vrf-target target:100:300;
 vrf-table-label;
}
```

---

## Verification

Confirm that the configuration is working properly.

- [Verifying Local IRB MACs on page 316](#)
- [Verifying Remote IRB MACs on page 317](#)
- [Verifying Local IRB IPs on page 318](#)
- [Verifying Remote IRB IPs on page 319](#)
- [Verifying CE-CE Inter-Subnet Forwarding on page 320](#)
- [Verifying CE-PE Inter-Subnet Forwarding on page 321](#)
- [Verifying PE-PE Inter-Subnet Forwarding on page 322](#)

### *Verifying Local IRB MACs*

**Purpose** Verify that the local IRB MACs are learned from L2ALD.

**Action** On Router PE1, determine the MAC address of the local IRB interface.

From operational mode, run the **show interfaces irb extensive | match "Current address"** command.



```

user@PE1> show interfaces irb extensive | match "Current address"
Current address: a8:d0:e5:54:0d:10, Hardware address: a8:d0:e5:54:0d:10

From operational mode, run the show route table evpn.0 extensive | find "a8:d0:e5:54:0d:10" command.

user@PE1> show route table evpn.0 extensive | find "a8:d0:e5:54:0d:10"
2:10.255.0.1:100::0::100::a8:d0:e5:54:0d:10/384 (1 entry, 1 announced)
TSI:
Page 0 idx 0, (group PE type Internal) Type 1 val 0x2736568 (adv_entry)
 Advertised metrics:
 Flags: Nexthop Change
 Nexthop: Self
 Localpref: 100
 AS path: [100] I
 Communities: target:100:100 evpn-default-gateway
Path 2:10.255.0.1:100::0::100::a8:d0:e5:54:0d:10 Vector len 4. Val: 0
 *EVPN Preference: 170
 Next hop type: Indirect
 Address: 0x26f8354
 Next-hop reference count: 6
 Protocol next hop: 10.255.0.1
 Indirect next hop: 0x0 - INH Session ID: 0x0
 State: <Active Int Ext>
 Age: 23:29:08
 Validation State: unverified
 Task: evpn-evpn
 Announcement bits (1): 1-BGP_RT_Background
 AS path: I
 Communities: evpn-default-gateway
 Route Label: 299776

```

**Meaning** The MAC-only route for the local IRB interface appears in the EVPN instance route table on Router PE1 and is learned from EVPN and tagged with the default gateway extended community.

#### *Verifying Remote IRB MACs*

**Purpose** Verify that the remote IRB MACs are learned from BGP.

**Action** On Router PE1, determine the MAC address of the local IRB interface.

From operational mode, run the **show interfaces irb extensive | match "Current address"** command.

```

user@PE1> show interfaces irb extensive | match "Current address"
Current address: a8:d0:e5:54:0d:10, Hardware address: a8:d0:e5:54:0d:10

```

On Router PE2, verify that the remote IRB MACs are learned.

From operational mode, run the **show route table evpn.0 extensive | find "a8:d0:e5:54:0d:10"** command.

```

user@PE2> show route table evpn.0 extensive | find "a8:d0:e5:54:0d:10"
2:10.255.0.1:100::0::100::a8:d0:e5:54:0d:10/384 (1 entry, 1 announced)
 *BGP Preference: 170/-101
 Route Distinguisher: 203.0.113.1:100
 Next hop type: Indirect

```

```

Address: 0x26f8d6c
Next-hop reference count: 10
Source: 10.255.0.1
Protocol next hop: 10.255.0.1
Indirect next hop: 0x2 no-forward INH Session ID: 0x0
State: <Secondary Active Int Ext>
Local AS: 100 Peer AS: 100
Age: 23:22:17 Metric2: 1
Validation State: unverified
Task: BGP_100.10.255.0.1
Announcement bits (1): 0-evpna-evpn
AS path: I
Communities: target:100:100 evpn-default-gateway
Import Accepted
Route Label: 299776
Localpref: 100
Router ID: 10.255.0.1
Primary Routing Table bgp.evpn.0
Indirect next hops: 1
 Protocol next hop: 10.255.0.1 Metric: 1
 Indirect next hop: 0x2 no-forward INH Session ID: 0x0
 Indirect path forwarding next hops: 1
 Next hop type: Router
 Next hop: 203.0.113.2 via ge-1/0/8.0
 Session Id: 0x1
 10.255.0.1/32 Originating RIB: inet.3
 Metric: 1 Node path count: 1
 Forwarding nexthops: 1
 Nexthop: 203.0.113.2 via ge-1/0/8.0

```

**Meaning** The MAC-only route for the remote IRB interface appears in the EVPN instance route table on Router PE2 and is learned from BGP and tagged with the default gateway extended community.

#### *Verifying Local IRB IPs*

**Purpose** Verify that the local IRB IPs are learned locally by RPD.

**Action** On Router PE1, determine the MAC and IP addresses of the local IRB interface.

From operational mode, run the **show interfaces irb extensive | match "Current address"** command.

```

user@PE1> show interfaces irb extensive | match "Current address"
Current address: a8:d0:e5:54:0d:10, Hardware address: a8:d0:e5:54:0d:10

```

From operational mode, run the **show interfaces irb.0 terse | match inet** command.

```

user@PE1> show interfaces irb.0 terse | match inet
irb.0 up up inet 10.0.0.251/24

```

From operational mode, run the **show route table evpn.evpn.0 extensive | find "a8:d0:e5:54:0d:10::10.0.0.251"** command.

```

user@PE2> show route table evpn.evpn.0 extensive | find "a8:d0:e5:54:0d:10::10.0.0.251"
2:10.255.0.1:100::0::100::a8:d0:e5:54:0d:10::10.0.0.251/384 (1 entry, 1 announced)
TSI:
Page 0 idx 0, (group PE type Internal) Type 1 val 0x27365a0 (adv_entry)

```

```

Advertised metrics:
 Flags: Nexthop Change
 Nexthop: Self
 Localpref: 100
 AS path: [100] I
 Communities: target:100:100 evpn-default-gateway
Path 2:10.255.0.1:100::0::100::a8:d0:e5:54:0d:10::10.0.0.251 Vector len 4. Val:
0
 *EVPN Preference: 170 <<<<<
 Next hop type: Indirect
 Address: 0x26f8354
 Next-hop reference count: 6
 Protocol next hop: 10.255.0.1
 Indirect next hop: 0x0 - INH Session ID: 0x0
 State: <Active Int Ext>
 Age: 23:48:46
 Validation State: unverified
 Task: evpna-evpn
 Announcement bits (1): 1-BGP_RT_Background
 AS path: I
 Communities: evpn-default-gateway
 Route Label: 299776

```

**Meaning** The MAC plus IP route for the local IRB interface appears in the EVPN instance route table on Router PE1 and is learned from EVPN and tagged with the default gateway extended community.

#### *Verifying Remote IRB IPs*

**Purpose** Verify that the remote IRB IPs are learned from BGP.

**Action** On Router PE1, determine the MAC and IP addresses of the local IRB interface.

From operational mode, run the **show interfaces irb extensive | match "Current address"** command.

```

user@PE1> show interfaces irb extensive | match "Current address"
Current address: a8:d0:e5:54:0d:10, Hardware address: a8:d0:e5:54:0d:10

```

From operational mode, run the **show interfaces irb.0 terse | match inet** command.

```

user@PE1> show interfaces irb.0 terse | match inet
irb.0 up up inet 10.0.0.251/24

```

On Router PE2, verify that the remote IRB IPs are learnt.

From operational mode, run the **show route table evpna.evpn.0 extensive | find "a8:d0:e5:54:0d:10::10.0.0.251"** command.

```

user@PE2> show route table evpna.evpn.0 extensive | find "a8:d0:e5:54:0d:10::10.0.0.251"
2:10.255.0.1:100::0::100::a8:d0:e5:54:0d:10::10.0.0.251/384 (1 entry, 1 announced)
 *BGP Preference: 170/-101
 Route Distinguisher: 203.0.113.2:100
 Next hop type: Indirect
 Address: 0x26f8d6c
 Next-hop reference count: 10
 Source: 10.255.0.1
 Protocol next hop: 10.255.0.1

```

```
Indirect next hop: 0x2 no-forward INH Session ID: 0x0
State: <Secondary Active Int Ext>
Local AS: 100 Peer AS: 100
Age: 23:56:36 Metric2: 1
Validation State: unverified
Task: BGP_100.10.255.0.1
Announcement bits (1): 0-evpna-evpn
AS path: I
Communities: target:100:100 evpn-default-gateway
Import Accepted
Route Label: 299776
Localpref: 100
Router ID: 10.255.0.1
Primary Routing Table bgp.evpn.0
Indirect next hops: 1
 Protocol next hop: 10.255.0.1 Metric: 1
 Indirect next hop: 0x2 no-forward INH Session ID: 0x0
 Indirect path forwarding next hops: 1
 Next hop type: Router
 Next hop: 203.0.113.2 via ge-1/0/8.0
 Session Id: 0x1
 10.255.0.1/32 Originating RIB: inet.3
 Metric: 1 Node path count: 1
 Forwarding nexthops: 1
 Nexthop: 203.0.113.2 via ge-1/0/8.0
```

**Meaning** The MAC plus IP route for the remote IRB interface appears in the EVPN instance route table on Router PE2 and is tagged with the default gateway extended community.

#### ***Verifying CE-CE Inter-Subnet Forwarding***

**Purpose** Verify inter-subnet forwarding between Routers CE1 and CE2.

**Action** From operational mode, run the **show route table inet.0** command.

```
user@CE1> show route table inet.0
inet.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0 *[Static/5] 00:15:09
 > to 10.0.0.251 via ge-1/1/7.0
10.0.0.0/24 *[Direct/0] 1d 23:24:30
 > via ge-1/1/7.0
10.0.0.1/32 *[Local/0] 1d 23:24:38
 Local via ge-1/1/7.0
```

From operational mode, run the **ping** command.

```
user@CE1> ping 192.0.2.0 interval 0.1 count 10
PING 192.0.2.0 (192.0.2.0): 56 data bytes
64 bytes from 192.0.2.0: icmp_seq=0 ttl=63 time=0.919 ms
64 bytes from 192.0.2.0: icmp_seq=1 ttl=63 time=0.727 ms
64 bytes from 192.0.2.0: icmp_seq=2 ttl=63 time=0.671 ms
64 bytes from 192.0.2.0: icmp_seq=3 ttl=63 time=0.671 ms
64 bytes from 192.0.2.0: icmp_seq=4 ttl=63 time=0.666 ms
64 bytes from 192.0.2.0: icmp_seq=5 ttl=63 time=0.704 ms
64 bytes from 192.0.2.0: icmp_seq=6 ttl=63 time=0.763 ms
64 bytes from 192.0.2.0: icmp_seq=7 ttl=63 time=0.750 ms
64 bytes from 192.0.2.0: icmp_seq=8 ttl=63 time=12.967 ms
64 bytes from 192.0.2.0: icmp_seq=9 ttl=63 time=0.752 ms

--- 192.0.2.0 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.666/1.959/12.967/3.670 ms
```

**Meaning** Ping from Router CE1 to Router CE2 is successful.

#### ***Verifying CE-PE Inter-Subnet Forwarding***

**Purpose** Verify inter-subnet forwarding between Routers CE1 and PE2.

**Action** From operational mode, run the **show route table inet.0** command.

```
user@CE1> show route table inet.0
inet.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0 *[Static/5] 00:15:09
 > to 10.0.0.251 via ge-1/1/7.0
10.0.0.0/24 *[Direct/0] 1d 23:24:30
 > via ge-1/1/7.0
10.0.0.1/32 *[Local/0] 1d 23:24:38
 Local via ge-1/1/7.0
```

From operational mode, run the **ping** command.

```
user@CE1> ping 192.0.2.5 interval 0.1 count 10
PING 192.0.2.5 (192.0.2.5): 56 data bytes
64 bytes from 192.0.2.5: icmp_seq=0 ttl=64 time=0.959 ms
64 bytes from 192.0.2.5: icmp_seq=1 ttl=64 time=0.710 ms
64 bytes from 192.0.2.5: icmp_seq=2 ttl=64 time=0.832 ms
64 bytes from 192.0.2.5: icmp_seq=3 ttl=64 time=0.754 ms
64 bytes from 192.0.2.5: icmp_seq=4 ttl=64 time=3.642 ms
64 bytes from 192.0.2.5: icmp_seq=5 ttl=64 time=0.660 ms
64 bytes from 192.0.2.5: icmp_seq=6 ttl=64 time=0.728 ms
64 bytes from 192.0.2.5: icmp_seq=7 ttl=64 time=0.725 ms
64 bytes from 192.0.2.5: icmp_seq=8 ttl=64 time=0.674 ms
64 bytes from 192.0.2.5: icmp_seq=9 ttl=64 time=0.760 ms

--- 192.0.2.5 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.666/1.959/12.967/3.670 ms
```

**Meaning** Ping from Router CE1 to Router PE2 is successful.

#### ***Verifying PE-PE Inter-Subnet Forwarding***

**Purpose** Verify inter-subnet forwarding between Routers PE1 and PE2.

**Action** From operational mode, run the **show route table vrf.inet.0 192.0.2.5** command.

```
user@PE1> show route table vrf.inet.0 192.0.2.5
vrf.inet.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.5/24 *[VRF/7] 02:24:32, metric2 1
 > to 10.0.0.2 via ge-1/0/8.0, Push 299776, Push 299776(top)
```

From operational mode, run the **ping** command.

```
user@CE1> ping routing-instance vrf.192.0.2.5 interval 0.1 count 10
PING 192.0.2.5 (192.0.2.5): 56 data bytes
64 bytes from 192.0.2.5: icmp_seq=0 ttl=64 time=9.613 ms
64 bytes from 192.0.2.5: icmp_seq=1 ttl=64 time=0.789 ms
64 bytes from 192.0.2.5: icmp_seq=2 ttl=64 time=0.803 ms
64 bytes from 192.0.2.5: icmp_seq=3 ttl=64 time=0.695 ms
64 bytes from 192.0.2.5: icmp_seq=4 ttl=64 time=0.742 ms
64 bytes from 192.0.2.5: icmp_seq=5 ttl=64 time=0.702 ms
64 bytes from 192.0.2.5: icmp_seq=6 ttl=64 time=0.725 ms
64 bytes from 192.0.2.5: icmp_seq=7 ttl=64 time=0.730 ms
64 bytes from 192.0.2.5: icmp_seq=8 ttl=64 time=0.713 ms
64 bytes from 192.0.2.5: icmp_seq=9 ttl=64 time=7.370 ms

--- 192.0.2.5 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.695/2.288/9.613/3.142 ms
```

**Meaning** Ping from Router PE1 to Router PE2's IRB interface is successful.





# Configuring EVPN with Support for Virtual Switch

- [Virtual Switch Support for EVPN Overview on page 325](#)
- [Configuring EVPN with Support for Virtual Switch on page 327](#)
- [Example: Configuring EVPN with Support for Virtual Switch on page 329](#)

## Virtual Switch Support for EVPN Overview

---

A Data Center Service Provider (DCSP) hosts the data center for its multiple customers onto a common physical network. To each customer (also called a tenant), the service looks like a full-fledged data center that can expand to 4094 VLANs and all private subnets. For disaster recovery, high availability, and optimization of resource utilization, it is common for the DCSP to span the data center to more than one site. When deploying the data center services, a DCSP faces the following main challenges:

- Extending Layer 2 domains across more than one data center site. This requires optimal intra-subnet traffic forwarding.
- Supporting optimal inter-subnet traffic forwarding and optimal routing in the event of virtual machine (VM) motion.
- Supporting multiple tenants with independent VLAN and subnet space.

Ethernet VPN is targeted to handle all of the above challenges, wherein:

- The basic EVPN functionality enables optimal intra-subnet traffic forwarding
- Implementing the integrated routing and bridging (IRB) solution in an EVPN deployment enables optimal inter-subnet traffic forwarding
- Configuring EVPN with virtual switch support enables multiple tenants with independent VLAN and subnet space

Because each data center hosts multiple tenants with independent VLAN and private subnet space, if an EVPN instance (EVI) was to stretch just one VLAN, it would be a severe problem to scale the data center services. In order to overcome this limitation, starting with Junos OS Release 14.1, a new service called the VLAN-aware bundling service is introduced. This feature provides the ability to extend Ethernet VLANs over a WAN

using a single EVPN instance while maintaining data-plane separation between the various VLANs associated with that instance.

Junos OS has a very flexible and scalable virtual switch interface. With virtual switch a single MX Series router can be divided into multiple logical switches. Layer 2 domains (also called bridge-domains) can be defined independently in each virtual switch. To achieve the VLAN-aware bundling service, an EVPN would be allowed to run in a virtual-switch routing instance.

A single EVPN instance can stretch up to 4094 bridge domains defined in a virtual switch to remote sites. A virtual switch can have more than 4094 bridge domains with a combination of none, single, and dual VLANs. However, because EVPN signaling deals only with single VLAN tags, only a maximum of 4094 bridge domains can be stretched. The EVPN virtual switch also provides support for trunk and access interfaces.

**NOTE:**

- The none VLAN option is not supported with bridge domains under the virtual switch instance type for EVPNs.
  - Dual VLANs are not supported with EVPN although they can be configured.
- 

There are two types of VLAN-aware bundling services:

- VLAN-aware bundling without translation

The service interface provides bundling of customer VLANs into a single Layer 2 VPN service instance with a guarantee for end-to-end customer VLAN transparency. The data-plane separation between the customer VLANs is maintained by creating a dedicated bridge-domain per VLAN.

- VLAN-aware bundling with translation

The service interface provides bundling of customer VLANs into a single Layer 2 VPN service instance. The data-plane separation between the customer VLANs is maintained by creating a dedicated bridge-domain per VLAN. The service interface supports customer VLAN translation to handle the scenario where different VLAN Identifiers (VIDs) are used on different interfaces to designate the same customer VLAN.

EVPN with virtual switch provides support for VLAN-aware bundling with translation only.

**Related Documentation**

- [Example: Configuring EVPN with Support for Virtual Switch on page 331](#)

## Configuring EVPN with Support for Virtual Switch

You can configure an Ethernet VPN (EVPN) with virtual switch support to enable multiple tenants with independent VLAN and subnet space within an EVPN instance. Virtual switch provides the ability to extend Ethernet VLANs over a WAN using a single EVPN instance while maintaining data-plane separation between the various VLANs associated with that instance. A single EVPN instance can stretch up to 4094 bridge domains defined in a virtual switch to remote sites.

When configuring virtual switch for EVPN, be aware of the following considerations:

- Due to default ARP policing, some of the ARP packets not destined for the device can be missed. This can lead to delayed ARP learning and synchronization.
- Clearing ARP for an EVPN can lead to inconsistency between the ARP table and the EVPN ARP table. To avoid this situation, clear both ARP and EVPN ARP tables.
- The **vlan-tag** can be configured for local switching. However, vlan-tagged VLANs should not be extended over the EVPN cloud.

Before you begin:

1. Configure the router interfaces.
2. Configure the router ID and autonomous system number for the device.
3. Enable chained composite next hop for EVPN.
4. Configure OSPF or any other IGP protocol.
5. Configure a BGP internal group.
6. Include the EVPN signaling network layer reachability information (NLRI) to the internal BGP group.
7. Configure RSVP or LDP.
8. Configure MPLS.
9. Create a label-switched path between the provider edge (PE) devices.

To configure the PE device:

1. Configure the virtual switch routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance instance-type virtual-switch
```

2. Configure the interface names for the virtual switch routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance interface interface-name
```

3. Configure the route distinguisher for the virtual switch routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance route-distinguisher route-distinguisher-value
```

4. Configure the VPN routing and forwarding (VRF) target community for the virtual switch routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance vrf-target vrf-target
```

5. List the VLAN identifiers that are to be EVPN extended.

```
[edit routing-instances]
user@PE1# set evpn-instance protocols evpn extended-vlan-list [vlan-id-range]
```

6. Configure the bridge domain for the first virtual switch routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance bridge-domains first-bridge-domain-name domain-type
bridge
```

7. Assign the VLAN ID for the first bridge domain.

```
[edit routing-instances]
user@PE1# set evpn-instance bridge-domains first-bridge-domain-name vlan-id 10
```

8. Configure the IRB interface as the routing interface for the first bridge domain.

```
[edit routing-instances]
user@PE1# set evpn-instance bridge-domains first-bridge-domain-name
routing-interface irb.0
```

9. Configure the interface name for the first bridge domain.

```
[edit routing-instances]
user@PE1# set evpn-instance bridge-domains first-bridge-domain-name bridge-options
interface CE-facing-interface
```

10. Configure the bridge domain for the second virtual switch routing instance.

```
[edit routing-instances]
user@PE1# set evpn-instance bridge-domains second-bridge-domain-name
domain-type bridge
```

11. Assign the VLAN ID for the second bridge domain.

```
[edit routing-instances]
user@PE1# set evpn-instance bridge-domains second-bridge-domain-name vlan-id
VLAN-ID
```

12. Configure the IRB interface as the routing interface for the second bridge domain.

```
[edit routing-instances]
user@PE1# set evpn-instance bridge-domains second-bridge-domain-name
routing-interface irb.1
```

13. Configure the interface name for the second bridge domain.

```
[edit routing-instances]
user@PE1# set evpn-instance bridge-domains second-bridge-domain-name
bridge-options interface CE-facing-interface
```

14. Configure the VRF routing instance.

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

15. Configure the IRB interface as the routing interface for the VRF routing instance.

```
[edit routing-instances]
user@PE1# set vrf-instance interface irb.0
user@PE1# set vrf-instance interface irb.1
```

16. Configure the route distinguisher for the VRF routing instance.

```
[edit routing-instances]
user@PE1# set vrf-instance route-distinguisher route-distinguisher-value
```

17. Configure the VRF target community for the VRF routing instance.

```
[edit routing-instances]
user@PE1# set vrf-instance vrf-target vrf-target
```

18. Configure the VRF label for the VRF routing instance.

```
[edit routing-instances]
user@PE1# set vrf-instance vrf-table-label
```

19. Verify and commit the configuration.

For example:

```
[edit routing-instances]
user@PE1# set evpna instance-type virtual-switch
user@PE1# set evpna interface ge-0/1/4.0
user@PE1# set evpna interface ge-0/1/4.1
user@PE1# set evpna route-distinguisher 10.255.169.37:1
user@PE1# set evpna vrf-target target:100:1
user@PE1# set evpna protocols evpn extended-vlan-list [10 20]
user@PE1# set evpna bridge-domains bda domain-type bridge
user@PE1# set evpna bridge-domains bda vlan-id 10
user@PE1# set evpna bridge-domains bda routing-interface irb.0
user@PE1# set evpna bridge-domains bda bridge-options interface ge-0/1/4.0
user@PE1# set evpna bridge-domains bdb domain-type bridge
user@PE1# set evpna bridge-domains bdb vlan-id 20
user@PE1# set evpna bridge-domains bdb routing-interface irb.1
user@PE1# set evpna bridge-domains bdb bridge-options interface ge-0/1/4.1
user@PE1# set vrf instance-type vrf
user@PE1# set vrf interface irb.0
user@PE1# set vrf interface irb.1
user@PE1# set vrf route-distinguisher 192.0.2.1:2
user@PE1# set vrf vrf-target target:100:2
user@PE1# set vrf vrf-table-label

[edit]
user@PE1# commit
commit complete
```

#### Related Documentation

- [Example: Configuring EVPN with Support for Virtual Switch on page 329](#)

## Example: Configuring EVPN with Support for Virtual Switch

- [Virtual Switch Support for EVPN Overview on page 330](#)
- [Example: Configuring EVPN with Support for Virtual Switch on page 331](#)

## Virtual Switch Support for EVPN Overview

A Data Center Service Provider (DCSP) hosts the data center for its multiple customers onto a common physical network. To each customer (also called a tenant), the service looks like a full-fledged data center that can expand to 4094 VLANs and all private subnets. For disaster recovery, high availability, and optimization of resource utilization, it is common for the DCSP to span the data center to more than one site. When deploying the data center services, a DCSP faces the following main challenges:

- Extending Layer 2 domains across more than one data center site. This requires optimal intra-subnet traffic forwarding.
- Supporting optimal inter-subnet traffic forwarding and optimal routing in the event of virtual machine (VM) motion.
- Supporting multiple tenants with independent VLAN and subnet space.

Ethernet VPN is targeted to handle all of the above challenges, wherein:

- The basic EVPN functionality enables optimal intra-subnet traffic forwarding
- Implementing the integrated routing and bridging (IRB) solution in an EVPN deployment enables optimal inter-subnet traffic forwarding
- Configuring EVPN with virtual switch support enables multiple tenants with independent VLAN and subnet space

Because each data center hosts multiple tenants with independent VLAN and private subnet space, if an EVPN instance (EVI) was to stretch just one VLAN, it would be a severe problem to scale the data center services. In order to overcome this limitation, starting with Junos OS Release 14.1, a new service called the VLAN-aware bundling service is introduced. This feature provides the ability to extend Ethernet VLANs over a WAN using a single EVPN instance while maintaining data-plane separation between the various VLANs associated with that instance.

Junos OS has a very flexible and scalable virtual switch interface. With virtual switch a single MX Series router can be divided into multiple logical switches. Layer 2 domains (also called bridge-domains) can be defined independently in each virtual switch. To achieve the VLAN-aware bundling service, an EVPN would be allowed to run in a virtual-switch routing instance.

A single EVPN instance can stretch up to 4094 bridge domains defined in a virtual switch to remote sites. A virtual switch can have more than 4094 bridge domains with a combination of none, single, and dual VLANs. However, because EVPN signaling deals only with single VLAN tags, only a maximum of 4094 bridge domains can be stretched. The EVPN virtual switch also provides support for trunk and access interfaces.

**NOTE:**

- The none VLAN option is not supported with bridge domains under the virtual switch instance type for EVPNs.
- Dual VLANs are not supported with EVPN although they can be configured.

There are two types of VLAN-aware bundling services:

- VLAN-aware bundling without translation

The service interface provides bundling of customer VLANs into a single Layer 2 VPN service instance with a guarantee for end-to-end customer VLAN transparency. The data-plane separation between the customer VLANs is maintained by creating a dedicated bridge-domain per VLAN.

- VLAN-aware bundling with translation

The service interface provides bundling of customer VLANs into a single Layer 2 VPN service instance. The data-plane separation between the customer VLANs is maintained by creating a dedicated bridge-domain per VLAN. The service interface supports customer VLAN translation to handle the scenario where different VLAN Identifiers (VIDs) are used on different interfaces to designate the same customer VLAN.

EVPN with virtual switch provides support for VLAN-aware bundling with translation only.

## Example: Configuring EVPN with Support for Virtual Switch

This example shows how to configure a virtual switch in an Ethernet VPN (EVPN) deployment.

- [Requirements on page 331](#)
- [Overview on page 332](#)
- [Configuration on page 332](#)
- [Verification on page 339](#)

### Requirements

This example uses the following hardware and software components:

- Two MX Series 3D Universal Edge Routers containing MPC FPCs.
- Two customer edge (CE) routers.
- Junos OS Release 14.1 or later.

Before you begin:

1. Configure the router interfaces.
2. Configure OSPF or any other IGP protocol.
3. Configure BGP.

4. Configure RSVP or LDP.
5. Configure MPLS.

## Overview

Starting with Junos OS Release 14.1, the Ethernet VPN (EVPN) solution on MX Series routers with MPC interfaces is extended to provide virtual switch support that enables multiple tenants with independent VLAN and subnet space within an EVPN instance. Virtual switch provides the ability to extend Ethernet VLANs over a WAN using a single EVPN instance while maintaining data-plane separation between the various VLANs associated with that instance. A single EVPN instance can stretch up to 4094 bridge domains defined in a virtual switch to remote sites.

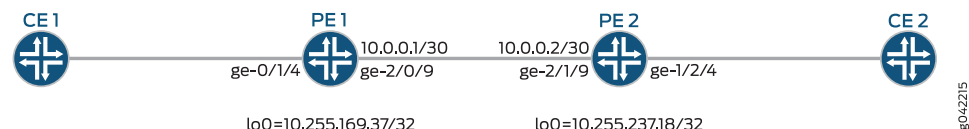
When configuring virtual switch for EVPN, be aware of the following considerations:

- Due to default ARP policing, some of the ARP packets not destined for the device can be missed. This can lead to delayed ARP learning and synchronization.
- Clearing ARP for an EVPN can lead to inconsistency between the ARP table and the EVPN ARP table. To avoid this situation, clear both ARP and EVPN ARP tables.
- The **vlan-tag** can be configured for local switching. However, vlan-tagged VLANs should not be extended over the EVPN cloud.

## Topology

Figure 26 on page 332 illustrates a simple EVPN topology with virtual switch support. Routers PE1 and PE2 are the provider edge (PE) routers that connect to one customer edge (CE) router each – CE1 and CE2.

Figure 26: EVPN with Virtual Switch Support



## 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 interfaces ge-2/0/9 unit 0 family inet address 10.0.0.1/30
 set interfaces ge-2/0/9 unit 0 family mpls
 set interfaces ge-0/1/4 flexible-vlan-tagging
 set interfaces ge-0/1/4 encapsulation flexible-ethernet-services
 set interfaces ge-0/1/4 unit 0 family bridge interface-mode trunk
 set interfaces ge-0/1/4 unit 0 vlan-id-list 10
 set interfaces ge-0/1/4 unit 1 family bridge interface-mode trunk
 set interfaces ge-0/1/4 unit 1 vlan-id-list 20
 set interfaces irb unit 0 family inet address 192.0.2.1/24
 set interfaces irb unit 1 family inet address 192.0.2.2/24
```



```

set interfaces lo0 unit 0 family inet address 10.255.169.37/32
set routing-options router-id 10.255.169.37
set routing-options autonomous-system 100
set routing-options forwarding-table chained-composite-next-hop ingress evpn
set protocols rsvp interface all
set protocols rsvp interface fxp0.0 disable
set protocols mpls label-switched-path PE1-to-PE2 from 10.255.169.37
set protocols mpls label-switched-path PE1-to-PE2 to 10.255.237.18
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 10.255.169.37
set protocols bgp group ibgp family evpn signaling
set protocols bgp group ibgp neighbor 10.255.237.18
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set routing-instances evpna instance-type virtual-switch
set routing-instances evpna interface ge-0/1/4.0
set routing-instances evpna interface ge-0/1/4.1
set routing-instances evpna route-distinguisher 10.255.169.37:1
set routing-instances evpna vrf-target target:100:1
set routing-instances evpna protocols evpn extended-vlan-list [10 20]
set routing-instances evpna bridge-domains bda domain-type bridge
set routing-instances evpna bridge-domains bda vlan-id 10
set routing-instances evpna bridge-domains bda routing-interface irb.0
set routing-instances evpna bridge-domains bda bridge-options interface ge-0/1/4.0
set routing-instances evpna bridge-domains bdb domain-type bridge
set routing-instances evpna bridge-domains bdb vlan-id 20
set routing-instances evpna bridge-domains bdb routing-interface irb.1
set routing-instances evpna bridge-domains bdb bridge-options interface ge-0/1/4.1
set routing-instances vrf instance-type vrf
set routing-instances vrf interface irb.0
set routing-instances vrf interface irb.1
set routing-instances vrf route-distinguisher 198.51.100.1:2
set routing-instances vrf vrf-target target:100:2
set routing-instances vrf vrf-table-label

```

```

PE2 set interfaces ge-2/1/9 unit 0 family inet address 10.0.0.2/30
set interfaces ge-2/1/9 unit 0 family mpls
set interfaces ge-1/2/4 flexible-vlan-tagging
set interfaces ge-1/2/4 encapsulation flexible-ethernet-services
set interfaces ge-1/2/4 unit 0 family bridge interface-mode trunk
set interfaces ge-1/2/4 unit 0 vlan-id-list 10
set interfaces ge-1/2/4 unit 1 family bridge interface-mode trunk
set interfaces ge-1/2/4 unit 1 vlan-id-list 20
set interfaces irb unit 0 family inet address 192.0.2.3/24
set interfaces irb unit 1 family inet address 192.0.2.4/24
set interfaces lo0 unit 0 family inet address 10.255.237.18/32
set routing-options router-id 10.255.237.18
set routing-options autonomous-system 100
set routing-options forwarding-table chained-composite-next-hop ingress evpn
set protocols rsvp interface all
set protocols rsvp interface fxp0.0 disable
set protocols mpls label-switched-path PE2-to-PE1 from 10.255.237.18
set protocols mpls label-switched-path PE2-to-PE1 to 10.255.169.37
set protocols mpls interface all

```

```

set protocols mpls interface fxp0.0 disable
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 10.255.237.18
set protocols bgp group ibgp family evpn signaling
set protocols bgp group ibgp neighbor 10.255.169.37
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set routing-instances evpna instance-type virtual-switch
set routing-instances evpna interface ge-1/2/4.0
set routing-instances evpna interface ge-1/2/4.1
set routing-instances evpna route-distinguisher 10.255.237.18:1
set routing-instances evpna vrf-target target:100:1
set routing-instances evpna protocols evpn extended-vlan-list [10 20]
set routing-instances evpna bridge-domains bda domain-type bridge
set routing-instances evpna bridge-domains bda vlan-id 10
set routing-instances evpna bridge-domains bda routing-interface irb.0
set routing-instances evpna bridge-domains bda bridge-options interface ge-1/2/4.0
set routing-instances evpna bridge-domains bdb domain-type bridge
set routing-instances evpna bridge-domains bdb vlan-id 20
set routing-instances evpna bridge-domains bdb routing-interface irb.1
set routing-instances evpna bridge-domains bdb bridge-options interface ge-1/2/4.1
set routing-instances vrf instance-type vrf
set routing-instances vrf interface irb.0
set routing-instances vrf interface irb.1
set routing-instances vrf route-distinguisher 198.51.100.2:2
set routing-instances vrf vrf-target target:100:2
set routing-instances vrf vrf-table-label

```

**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 Router PE1:



**NOTE:** Repeat this procedure for Router PE2, after modifying the appropriate interface names, addresses, and other parameters.

1. Configure the PE1 interfaces.

**[edit interfaces]**

```

user@PE1# set ge-2/0/9 unit 0 family inet address 10.0.0.1/30
user@PE1# set ge-2/0/9 unit 0 family mpls

```

```

user@PE1# set ge-0/1/4 flexible-vlan-tagging
user@PE1# set ge-0/1/4 encapsulation flexible-ethernet-services
user@PE1# set ge-0/1/4 unit 0 family bridge interface-mode trunk
user@PE1# set ge-0/1/4 unit 0 vlan-id-list 10
user@PE1# set ge-0/1/4 unit 1 family bridge interface-mode trunk
user@PE1# set ge-0/1/4 unit 1 vlan-id-list 20

```

```

user@PE1# set irb unit 0 family inet address 192.0.2.1/24
user@PE1# set irb unit 1 family inet address 192.0.2.2/24

```

- ```

user@PE1# set lo0 unit 0 family inet address 10.255.169.37/32

```
2. Set the router ID and autonomous system number for Router PE1.


```

[edit routing-options]
user@PE1# set router-id 10.255.169.37
user@PE1# set autonomous-system 100

```
 3. Configure the chained composite next hop for EVPN.


```

[edit routing-options]
user@PE1# set forwarding-table chained-composite-next-hop ingress evpn

```
 4. Enable RSVP on all the interfaces of Router PE1, excluding the management interface.


```

[edit protocols]
user@PE1# set rsvp interface all
user@PE1# set rsvp interface fxp0.0 disable

```
 5. Create label-switched paths for PE1 to reach PE2.


```

[edit protocols]
user@PE1# set mpls label-switched-path PE1-to-PE2 from 10.255.169.37
user@PE1# set mpls label-switched-path PE1-to-PE2 to 10.255.237.18

```
 6. Enable MPLS on all the interfaces of Router PE1, excluding the management interface.


```

[edit protocols]
user@PE1# set mpls interface all
user@PE1# set mpls interface fxp0.0 disable

```
 7. Configure the BGP group for Router PE1.


```

[edit protocols]
user@PE1# set bgp group ibgp type internal

```
 8. Assign local and neighbor addresses to the ibgp BGP group for Router PE1 to peer with Router PE2.


```

[edit protocols]
user@PE1# set bgp group ibgp local-address 10.255.169.37
user@PE1# set bgp group ibgp neighbor 10.255.237.18

```
 9. Include the EVPN signaling Network Layer Reachability Information (NLRI) to the ibgp BGP group.


```

[edit protocols]
user@PE1# set bgp group ibgp family evpn signaling

```
 10. Configure OSPF on all the interfaces of Router PE1, excluding the management interface.


```

[edit protocols]
user@PE1# set ospf area 0.0.0.0 interface all
user@PE1# set ospf area 0.0.0.0 interface fxp0.0 disable

```
 11. Configure the virtual switch routing instance.


```

[edit routing-instances]
user@PE1# set evpna instance-type virtual-switch

```

12. Configure the interface name for the evpna routing instance.

```
[edit routing-instances]
user@PE1# set evpna interface ge-0/1/4.0
user@PE1# set evpna interface ge-0/1/4.1
```
13. Configure the route distinguisher for the evpna routing instance.

```
[edit routing-instances]
user@PE1# set evpna route-distinguisher 10.255.169.37:1
```
14. Configure the VPN routing and forwarding (VRF) target community for the evpna routing instance.

```
[edit routing-instances]
user@PE1# set evpna vrf-target target:100:1
```
15. List the VLAN identifiers that are to be EVPN extended.

```
[edit routing-instances]
user@PE1# set evpna protocols evpn extended-vlan-list [ 10 20 ]
```
16. Configure the bridge domains for the evpna routing instance.

```
[edit routing-instances]
user@PE1# set evpna bridge-domains bda domain-type bridge
```
17. Assign the VLAN ID for the bda bridge domain.

```
[edit routing-instances]
user@PE1# set evpna bridge-domains bda vlan-id 10
```
18. Configure the IRB interface as the routing interface for the bda bridge domain.

```
[edit routing-instances]
user@PE1# set evpna bridge-domains bda routing-interface irb.0
```
19. Configure the interface name for the bda bridge domain.

```
[edit routing-instances]
user@PE1# set evpna bridge-domains bda bridge-options interface ge-0/1/4.0
```
20. Configure the bridge domains for the evpna routing instance.

```
[edit routing-instances]
user@PE1# set evpna bridge-domains bdb domain-type bridge
```
21. Assign the VLAN ID for the bdb bridge domain.

```
[edit routing-instances]
user@PE1# set evpna bridge-domains bdb vlan-id 20
```
22. Configure the IRB interface as the routing interface for the bda bridge domain.

```
[edit routing-instances]
user@PE1# set evpna bridge-domains bdb routing-interface irb.1
```
23. Configure the interface name for bdb bridge domain.

```
[edit routing-instances]
user@PE1# set evpna bridge-domains bdb bridge-options interface ge-0/1/4.1
```
24. Configure the VRF routing instance.

```
[edit routing-instances]
```

```
user@PE1# set vrf instance-type vrf
```

25. Configure the IRB interface as the routing interface for the vrf routing instance.

```
[edit routing-instances]
user@PE1# set vrf interface irb.0
user@PE1# set vrf interface irb.1
```

26. Configure the route distinguisher for the vrf routing instance.

```
[edit routing-instances]
user@PE1# set vrf route-distinguisher 198.51.100.1:2
```

27. Configure the VRF target community for the vrf routing instance.

```
[edit routing-instances]
user@PE1# set vrf vrf-target target:100:2
```

28. Configure VRF label for the vrf routing instance.

```
[edit routing-instances]
user@PE1# set vrf vrf-table-label
```

Results

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

```
user@PE1# show interfaces
ge-2/0/9 {
  unit 0 {
    family inet {
      address 10.0.0.1/30;
    }
    family mpls;
  }
}
ge-0/1/4 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 0 {
    family bridge {
      interface-mode trunk;
      vlan-id-list 10;
    }
  }
  unit 1 {
    family bridge {
      interface-mode trunk;
      vlan-id-list 20;
    }
  }
}
irb {
  unit 0 {
    family inet {
```

```
        address 192.0.2.1/24;
    }
}
unit 1 {
    family inet {
        address 192.0.2.2/24;
    }
}
}
lo0 {
    unit 0 {
        family inet {
            address 10.255.169.37/32;
        }
    }
}

user@PE1# show routing-options
router-id 10.255.169.37;
autonomous-system 100;
forwarding-table {
    chained-composite-next-hop {
        ingress {
            evpn;
        }
    }
}

user@PE1# show protocols
rsvp {
    interface all;
    interface fxp0.0 {
        disable;
    }
}
mpls {
    label-switched-path PE1-to-PE2 {
        from 10.255.169.37;
        to 10.255.237.18;
    }
    interface all;
    interface fxp0.0 {
        disable;
    }
}
bgp {
    group ibgp {
        type internal;
        local-address 10.255.169.37;
        family evpn {
            signaling;
        }
        neighbor 10.255.237.18;
    }
}
ospf {
    area 0.0.0.0 {
```

```

    interface all;
    interface fxp0.0 {
        disable;
    }
}
}

user@PE1# show routing-instances
evpna {
    instance-type virtual-switch;
    interface ge-0/1/4.0;
    interface ge-0/1/4.1;
    route-distinguisher 10.255.169.37:1;
    vrf-target target:100:1;
    protocols {
        evpn {
            extended-vlan-list [ 10 20 ];
        }
    }
    bridge-domains {
        bda {
            domain-type bridge;
            vlan-id 10;
            routing-interface irb.0;
            bridge-options {
                interface ge-0/1/4.0;
            }
        }
        bdb {
            domain-type bridge;
            vlan-id 20;
            routing-interface irb.1;
            bridge-options {
                interface ge-0/1/4.1;
            }
        }
    }
}
vrf {
    instance-type vrf;
    interface irb.0;
    interface irb.1;
    route-distinguisher 10.255.169.37:2;
    vrf-target target:100:2;
    vrf-table-label;
}

```

Verification

Confirm that the configuration is working properly.

- [Verifying the Bridge Domain Configuration on page 340](#)
- [Verifying MAC Table Routes on page 340](#)
- [Verifying the Bridge EVPN Peer Gateway MAC on page 341](#)

Verifying the Bridge Domain Configuration

Purpose Verify the bridge domain configuration for the evpna routing instance.

Action From operational mode, run the **show bridge domain extensive** command.

```

user@PE1> show bridge domain extensive
Routing instance: evpna
Bridge domain: bda                               State: Active
Bridge VLAN ID: 10                               EVPN extended: Yes
Interfaces:
  ge-0/1/4.0
  pip-10.000010000000
  pip-10.fe0f0f000000
Total MAC count: 2

Bridge domain: bdb                               State: Active
Bridge VLAN ID: 20                               EVPN extended: Yes
Interfaces:
  ge-0/1/4.1
  pip-11.010010000000
  pip-11.ffff0f000000
Total MAC count: 2

```

Meaning The configured bridge domains **bda** and **bdb** and their associated VLAN IDs and interfaces are displayed. The bridge domains are also extended with EVPN.

Verifying MAC Table Routes

Purpose Verify the MACs learned in the data plane and control plane.

Action From operational mode, run the **show bridge mac-table** command.

```

user@PE1> show bridge mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
          SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : evpna
Bridging domain : bda, VLAN : 10
  MAC          MAC      Logical   NH      RTR
  address      flags    interface Index  ID
  00:00:00:aa:01:01  S      ge-0/1/4.0
  00:00:00:bb:01:01  DC
  00:00:00:cc:01:01  DC
                                1048574 1048574
                                1048576 1048576

Bridging domain : bdb, VLAN : 20
  MAC          MAC      Logical   NH      RTR
  address      flags    interface Index  ID
  00:00:00:aa:02:01  S      ge-0/1/4.1
  00:00:00:bb:02:01  DC
  00:00:00:cc:02:01  DC
                                1048575 1048575
                                1048577 1048577

```

Meaning The configured static MACs for the bridge domains are displayed.

Verifying the Bridge EVPN Peer Gateway MAC

Purpose Verify the bridge EVPN peer gateway MAC for the evpna routing instance.

Action From operational mode, run the **show bridge evpn peer-gateway-macs** command.

```
user@PE1> show bridge evpn peer-gateway-macs
Routing instance : evpna
  Bridging domain : bda, VLAN : 10
    Installed GW MAC addresses:
      00:23:9c:96:af:f0
      a8:d0:e5:5b:02:08

  Bridging domain : bdb, VLAN : 20
    Installed GW MAC addresses:
      00:23:9c:96:af:f0
      a8:d0:e5:5b:02:08
```

Meaning The gateway MACs of the EVPN peers for the evpna routing instance are displayed.

PART 5

Configuring Layer 2 Circuits

- [Overview on page 345](#)
- [Layer 2 Circuits Configuration Overview on page 347](#)
- [Configuring Class of Service with Layer 2 Circuits on page 361](#)
- [Configuring Pseudowire Redundancy for Layer 2 Circuits on page 367](#)
- [Configuring Load Balancing for Layer 2 Circuits on page 395](#)
- [Configuring Protection Features for Layer 2 Circuits on page 399](#)
- [Monitoring Layer 2 Circuits with BFD on page 433](#)
- [Troubleshooting Layer 2 Circuits on page 443](#)

Overview

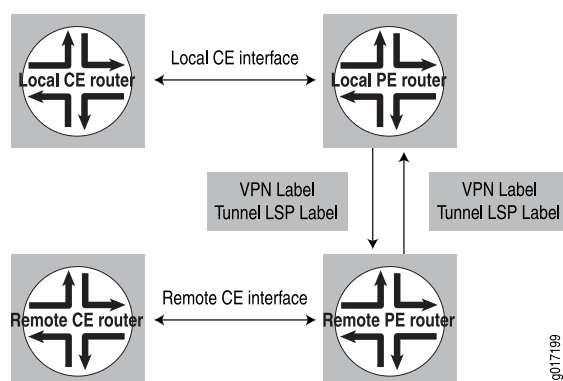
- [Layer 2 Circuit Overview on page 345](#)

Layer 2 Circuit Overview

A Layer 2 circuit is a point-to-point Layer 2 connection transported using Multiprotocol Label Switching (MPLS) or other tunneling technology on the service provider's network. A Layer 2 circuit is similar to a circuit cross-connect (CCC), except that multiple virtual circuits (VCs) are transported over a single shared label-switched path (LSP) tunnel between two provider edge (PE) routers. In contrast, each CCC requires a separate dedicated LSP.

The Junos OS implementation of Layer 2 circuits supports only the remote form of a Layer 2 circuit; that is, a connection from a local customer edge (CE) router to a remote CE router. [Figure 27 on page 345](#) illustrates the components of a Layer 2 circuit.

Figure 27: Components of a Layer 2 Circuit



To establish a Layer 2 circuit, the Link Integrity Protocol (LIP) is used as the signaling protocol to advertise the ingress label to the remote PE routers. For this purpose, a targeted remote LDP neighbor session is established using the extended discovery mechanism described in LDP, and the session is brought up to the remote PE loopback IP address. Because LDP looks at the Layer 2 circuit configuration and initiates extended neighbor discovery for all the Layer 2 circuit neighbors (the remote PEs), no new configuration is necessary in LDP. Each Layer 2 circuit is represented by the logical interface connecting the local PE router to the local customer edge (CE) router. Note that LDP

must be enabled on the lo0.0 interface for extended neighbor discovery to function correctly.

Packets are sent to remote CE routers over an egress VPN label advertised by the remote PE router, using a targeted LDP session. The VPN label is sent over an LDP LSP to the remote PE router connected to the remote CE router. Return traffic from the remote CE router destined to the local CE router is sent using an ingress VPN label advertised by the local PE router, which is also sent over the LDP LSP to the local PE router from the remote PE router.

**Related
Documentation**

- *Understanding Layer 3 VPNs*
- [Layer 2 VPN Applications on page 122](#)
- [Applications for Interconnecting a Layer 2 Circuit with a Layer 2 Circuit on page 990](#)
- [Applications for Interconnecting a Layer 2 Circuit with a Layer 3 VPN on page 1015](#)
- [Example: Interconnecting a Layer 2 Circuit with a Layer 2 Circuit on page 999](#)
- [Example: Interconnecting a Layer 2 Circuit with a Layer 3 VPN on page 1015](#)
- [Example: Interconnecting a Layer 2 Circuit with a Layer 2 VPN on page 991](#)

Layer 2 Circuits Configuration Overview

- [Configuring Static Layer 2 Circuits on page 347](#)
- [Configuring Local Interface Switching in Layer 2 Circuits on page 348](#)
- [Configuring Interfaces for Layer 2 Circuits on page 350](#)
- [Configuring Policies for Layer 2 Circuits on page 357](#)
- [Configuring LDP for Layer 2 Circuits on page 360](#)

Configuring Static Layer 2 Circuits

You can configure static Layer 2 circuit pseudowires. Static pseudowires are designed for networks that do not support LDP or do not have LDP enabled. You configure a static pseudowire by configuring static values for the in and out labels needed to enable a pseudowire connection. The **ignore-mtu-mismatch**, **ignore-vlan-id**, and **ignore-encapsulation-mismatch** statements are not relevant for static pseudowire configurations since the peer router cannot forward this information.

When you configure static pseudowires, you need to manually compare the encapsulation, TDM bit rate, and control word of the router with the remote peer router and ensure that they match, otherwise the static pseudowire might not work.

To configure static Layer 2 circuit pseudowires, include the **static** statement:

```
static {  
    incoming-label label;  
    outgoing-label label;  
    send-oam;  
}
```

For a list of hierarchy levels at which you can configure this statement, see the statement summary section for this statement.

You can configure a static pseudowire as a standalone Layer 2 circuit or in conjunction with a redundant pseudowire. You configure the static pseudowire statement at the **[edit protocols l2circuit neighbor address interface *interface-name*]** hierarchy level. You configure the redundant pseudowire at the **[edit protocols l2circuit neighbor address interface *interface-name* backup-neighbor *neighbor*]** hierarchy level. If you configure a static pseudowire to a neighbor and also configure a redundant pseudowire, the redundant pseudowire must also be static.

You can enable the ability to ping a static pseudowire by configuring the **send-oam** statement. This functionality applies to the backup neighbor as well. Once you have configured this statement, you can ping the static pseudowire by issuing the **ping mpls l2circuit** command.

For information about how to configure redundant pseudowires, see “[Configuring Redundant Pseudowires for Layer 2 Circuits and VPLS](#)” on page 179.

**Related
Documentation**

- [Configuring Redundant Pseudowires for Layer 2 Circuits and VPLS on page 179](#)
- [ping mpls l2circuit on page 1244](#)

Configuring Local Interface Switching in Layer 2 Circuits

You can configure a virtual circuit entirely on the local router, terminating the circuit on a local interface. Possible uses for this feature include being able to enable switching between Frame Relay DLCIs.

To configure a virtual circuit to terminate locally, include the **local-switching** statement:

```
local-switching {  
  interface interface-name {  
    description text;  
    end-interface {  
      interface interface-name;  
      no-revert;  
      protect-interface interface-name;  
    }  
    ignore-mtu-mismatch;  
    no-revert;  
    protect-interface interface-name;  
  }  
}
```

You can include this statement at the following hierarchy levels:

- **[edit protocols l2circuit]**
- **[edit logical-systems *logical-system-name* protocols l2circuit]**

The following sections describe how to configure local interface switching:

- [Configuring the Interfaces for the Local Interface Switch on page 348](#)
- [Enabling Local Interface Switching When the MTU Does Not Match on page 349](#)

Configuring the Interfaces for the Local Interface Switch

Local interface switching requires you to configure at least two interfaces:

- Starting interface—Include the **interface** statement at the **[edit protocols l2circuit local-switching]** hierarchy level.
- Ending interface—Include the **end-interface** statement at the **[edit protocols l2circuit local-switching interface *interface-name*]** hierarchy level.

You can also configure virtual circuit interface protection for each local interface:

- Protect interface for the starting interface—Include the **protect-interface** statement at the **[edit protocols l2circuit local-switching interface *interface-name*]** hierarchy level.
- Protect interface for the ending interface—Include the **protect-interface** statement at the **[edit protocols l2circuit local-switching interface *interface-name* end-interface]** hierarchy level.

For more information about how to configure protect interfaces, see [“Configuring the Protect Interface” on page 353](#).

Typically, when the primary interface goes down, the pseudowire starts using the protect interface. By default, when the primary interface comes back online, the interface is switched-over back from the protect interface to the primary interface. To prevent the switchover back to the primary interface, unless the primary interface goes down, include the **no-revert** statement. This prevents loss of traffic during the switchover.



NOTE: If the protect interface fails, the interface is switched-over back to the primary interface, irrespective of whether or not the **no-revert** statement is included in the configuration.

You can configure the **no-revert** statement both for the starting interface and the ending interface.

```
[edit protocols l2circuit local-switching interface interface-name]
no-revert;
end-interface {
  interface interface-name;
  no-revert;
}
```



NOTE: The protect interface must be configured prior to configuring the **no-revert** statement.

Enabling Local Interface Switching When the MTU Does Not Match

You can configure a local switching interface to ignore the MTU configuration set for the associated physical interface. This enables you to bring up a circuit between two logical interfaces that are defined on physical interfaces with different MTU values.

To configure the local switching interface to ignore the MTU configured for the physical interface, include the **ignore-mtu-mismatch** statement:

```
ignore-mtu-mismatch;
```

You can include this statement at the following hierarchy levels:

- **[edit protocols l2circuit local-switching interface *interface-name*]**

- [edit logical-systems *logical-system-name* protocols l2circuit local-switching interface *interface-name*]

Configuring Interfaces for Layer 2 Circuits

The following sections describe how to configure interfaces for Layer 2 circuits:

- [Configuring the Address for the Neighbor of the Layer 2 Circuit on page 350](#)
- [Configuring the Neighbor Interface for the Layer 2 Circuit on page 350](#)
- [Configuring the Interface Encapsulation Type for Layer 2 Circuits on page 356](#)
- [Configuring ATM2 IQ Interfaces for Layer 2 Circuits on page 357](#)

Configuring the Address for the Neighbor of the Layer 2 Circuit

All the Layer 2 circuits using a particular remote PE router designated for remote CE routers are listed under the **neighbor** statement (“neighbor” designates the PE router). Each neighbor is identified by its IP address and is usually the end-point destination for the label-switched path (LSP) tunnel transporting the Layer 2 circuit.

To configure a PE router as a neighbor for a Layer 2 circuit, specify the neighbor address using the **neighbor** statement:

```
neighbor address {  
  ...  
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols l2circuit]
- [edit logical-systems *logical-system-name* protocols l2circuit]

Configuring the Neighbor Interface for the Layer 2 Circuit

Each Layer 2 circuit is represented by the logical interface connecting the local provider edge (PE) router to the local customer edge (CE) router. This interface is tied to the Layer 2 circuit neighbor configured in [“Configuring the Address for the Neighbor of the Layer 2 Circuit” on page 350](#).

To configure the interface for a Layer 2 circuit neighbor, include the **interface** statement:



NOTE: The commit operation fails, if the same logical interface is configured for both Layer 2 circuit and ccc connection.

```
interface interface-name {  
  bandwidth (bandwidth | ctnumber bandwidth);  
  community community-name;  
  (control-word | no-control-word);  
  description text;  
  encapsulation-type type;  
  ignore-encapsulation-mismatch;  
  ignore-mtu-mismatch;
```

```

mtu mtu-number;
no-revert;
protect-interface interface-name;
pseudowire-status-tlv;
psn-tunnel-endpoint address;
virtual-circuit-id identifier;
}

```

You can include this statement at the following hierarchy levels:

- [edit protocols l2circuit neighbor *address*]
- [edit logical-systems *logical-system-name* protocols l2circuit neighbor *address*]

The following sections describe how to configure the interface for the Layer 2 circuit neighbor:

- [Configuring a Community for the Layer 2 Circuit on page 351](#)
- [Configuring the Control Word for Layer 2 Circuits on page 351](#)
- [Configuring the Encapsulation Type for the Layer 2 Circuit Neighbor Interface on page 353](#)
- [Enabling the Layer 2 Circuit When the Encapsulation Does Not Match on page 353](#)
- [Configuring the Protect Interface on page 353](#)
- [Configuring the Protect Interface From Switching Over to the Primary Interface on page 354](#)
- [Configuring the Pseudowire Status TLV on page 354](#)
- [Configuring Layer 2 Circuits over Both RSVP and LDP LSPs on page 355](#)
- [Configuring the Virtual Circuit ID on page 356](#)

Configuring a Community for the Layer 2 Circuit

To configure a community for a Layer 2 circuit, include the **community** statement:

```
community community-name;
```

You can include this statement at the following hierarchy levels:

- [edit protocols l2circuit neighbor *address* interface *interface-name*]
- [edit logical-systems *logical-system-name* protocols l2circuit neighbor *address* interface *interface-name*]

For information about how to configure a routing policy for a Layer 2 circuit, see [“Configuring Policies for Layer 2 Circuits” on page 357](#).

Configuring the Control Word for Layer 2 Circuits

To emulate the virtual circuit (VC) encapsulation for Layer 2 circuits, a 4-byte control word is added between the Layer 2 protocol data unit (PDU) being transported and the VC label that is used for demultiplexing. For most protocols, a null control word consisting of all zeroes is sent between Layer 2 circuit neighbors.

However, individual bits are available in a control word that can carry Layer 2 protocol control information. The control information is mapped into the control word, which

allows the header of a Layer 2 protocol to be stripped from the frame. The remaining data and control word can be sent over the Layer 2 circuit, and the frame can be reassembled with the proper control information at the egress point of the circuit.

The following Layer 2 protocols map Layer 2 control information into special bit fields in the control word:

- **Frame Relay**—The control word supports the transport of discard eligible (DE), forward explicit congestion notification (FECN), and backward explicit congestion notification (BECN) information. For configuration information, see [“Configuring the Control Word for Frame Relay Interfaces” on page 352](#).



NOTE: Frame Relay is not supported on the ACX Series routers.

- **ATM AAL5 mode**—The control word supports the transport of sequence number processing, ATM cell loss priority (CLP), and explicit forward congestion indication (EFCI) information. When you configure an AAL5 mode Layer 2 circuit, the control information is carried by default and no additional configuration is needed.
- **ATM cell-relay mode**—The control word supports sequence number processing only. When you configure a cell-relay mode Layer 2 circuit, the sequence number information is carried by default and no additional configuration is needed.

The Junos OS implementation of sequence number processing for ATM cell-relay mode and AAL5 mode is not the same as that described in Sec. 3.1.2 of the IETF draft *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*. The differences are as follows:

- A packet with a sequence number of 0 is considered as out of sequence.
- A packet that does not have the next incremental sequence number is considered out of sequence.
- When out-of-sequence packets arrive, the sequence number in the Layer 2 circuit control word increments by one and becomes the expected sequence number for the neighbor.

The following sections discuss how to configure the control word for Layer 2 circuits:

- [Configuring the Control Word for Frame Relay Interfaces on page 352](#)
- [Disabling the Control Word for Layer 2 Circuits on page 353](#)

Configuring the Control Word for Frame Relay Interfaces

On interfaces with Frame Relay CCC encapsulation, you can configure Frame Relay control bit translation to support Frame Relay services over IP and MPLS backbones by using CCC, Layer 2 VPNs, and Layer 2 circuits. When you configure translation of Frame Relay control bits, the bits are mapped into the Layer 2 circuit control word and preserved across the IP or MPLS backbone.

For information about how to configure the control bits, see the *Junos OS Network Interfaces Library for Routing Devices* and the *Junos OS, Release 15.1*.

Disabling the Control Word for Layer 2 Circuits

The Junos OS can typically determine whether a neighboring router supports the control word. However, if you want to explicitly disable its use on a specific interface, include the **no-control-word** statement:

```
no-control-word;
```

For a list of hierarchy levels at which you can configure this statement, see the statement summary section for this statement.

Configuring the Encapsulation Type for the Layer 2 Circuit Neighbor Interface

You can specify the Layer 2 circuit encapsulation type for the interface receiving traffic from a Layer 2 circuit neighbor. The encapsulation type is carried in the LDP-signaling messages exchanged between Layer 2 circuit neighbors when pseudowires are created. The encapsulation type you configure for each Layer 2 circuit neighbor varies depending on the type of networking equipment or the type of Layer 2 protocol you have deployed in your network. If you do not specify an encapsulation type for the Layer 2 circuit, the encapsulation of the CE device interface is used by default.

Specify the encapsulation type for the Layer 2 circuit neighbor interface by including the **encapsulation-type** statement:

```
encapsulation-type (atm-aal5 | atm-cell | atm-cell-port-mode | atm-cell-vc-mode |
atm-cell-vp-mode | cesop | cisco-hdlc | ethernet | ethernet-vlan | frame-relay |
frame-relay-port-mode | interworking | ppp | satop-e1 | satop-e3 | satop-t1 | satop-t3);
```

You can include this statement at the following hierarchy levels:

- **[edit protocols l2circuit neighbor address interface *interface-name*]**
- **[edit logical-systems *logical-system-name* protocols l2circuit neighbor address interface *interface-name*]**

Enabling the Layer 2 Circuit When the Encapsulation Does Not Match

You can configure the Junos OS to allow a Layer 2 circuit to be established even though the encapsulation configured on the CE device interface does not match the encapsulation configured on the Layer 2 circuit interface by including the **ignore-encapsulation-mismatch** statement. You can configure the **ignore-encapsulation-mismatch** statement for the connection to the remote connection by including the statement at the **[edit protocols l2circuit neighbor address interface *interface-name*]** hierarchy level or for the local connection by including this statement at the **[edit protocols l2circuit local-switching interface *interface-name*]** hierarchy level.

```
ignore-encapsulation-mismatch;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring the Protect Interface

You can configure a protect interface for the logical interface linking a virtual circuit to its destination, whether the destination is remote or local. A protect interface provides

a backup for the protected interface in case of failure. Network traffic uses the primary interface only so long as the primary interface functions. If the primary interface fails, traffic is switched to the protect interface. The protect interface is optional.

To configure the protect interface, include the **protect-interface** statement:

```
protect-interface interface-name;
```



NOTE: The protect interface must be configured prior to configuring the **no-revert** statement.

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

For an example of how to configure a protect interface for a Layer 2 circuit, see “[Example: Configuring Layer 2 Circuit Protect Interfaces](#)” on page 415.

Configuring the Protect Interface From Switching Over to the Primary Interface

Typically, when the primary interface goes down, the pseudowire starts using the protect interface. By default, when the primary interface comes back online, the interface is switched-over back from the protect interface to the primary interface. To prevent the switchover back to the primary interface, unless the protect interface goes down, include the **no-revert** statement. This prevents loss of traffic during the switchover.



NOTE: If the protect interface fails, the interface is switched-over back to the primary interface, irrespective of whether or not the **no-revert** statement is included in the configuration.

You can configure the **no-revert** statement at the **[edit protocols l2circuit neighbor address interface *interface-name*]** hierarchy level:

```
[edit protocols l2circuit neighbor address interface interface-name]  
no-revert;
```

Configuring the Pseudowire Status TLV

The pseudowire status type length variable (TLV) is used to communicate the status of a pseudowire back and forth between two PE routers. For Layer 2 circuit configurations, you can configure the PE router to negotiate the pseudowire with its neighbor using the pseudowire status TLV. This same functionality is also available for LDP VPLS neighbor configurations. The pseudowire status TLV is configurable for each pseudowire connection and is disabled by default. The pseudowire status negotiation process assures that a PE router reverts back to the label withdraw method for pseudowire status if its remote PE router neighbor does not support the pseudowire status TLV.

Unlike the control word, a PE router’s ability to support the pseudowire status TLV is communicated when the initial label mapping message is sent to its remote PE router. Once the PE router transmits its support for the pseudowire status TLV to its remote PE router, it includes the pseudowire status TLV in every label mapping message sent to

the remote PE router. If you disable support for the pseudowire status TLV on the PE router, a label withdraw message is sent to the remote PE router and then a new label mapping message without the pseudowire status TLV follows.

To configure the pseudowire status TLV for the pseudowire to the neighbor PE router, include the **pseudowire-status-tlv** statement:

```
pseudowire-status-tlv;
```

For a list of the hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring Layer 2 Circuits over Both RSVP and LDP LSPs

You can configure two Layer 2 circuits between the same two routers, and have one Layer 2 circuit traverse an RSVP LSP and the other traverse an LDP LSP. To accomplish this, you need to configure two loopback addresses on the local router. You configure one of the loopback address for the Layer 2 circuit traversing the RSVP LSP. You configure the other loopback address to handle the Layer 2 circuit traversing the LDP LSP. For information about how to configure multiple loop back interfaces, see *Configuring Logical Units on the Loopback Interface for Routing Instances in Layer 3 VPNs*.

You also need to configure a packet switched network (PSN) tunnel endpoint for one of the Layer 2 circuits. It can be either the Layer 2 circuit traversing the RSVP LSP or the one traversing the LDP LSP. The PSN tunnel endpoint address is the destination address for the LSP on the remote router.

To configure the address for the PSN tunnel endpoint, include the **psn-tunnel-endpoint** statement:

```
psn-tunnel-endpoint address;
```

You can include this statement at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols l2circuit neighbor *address* interface *interface-name*]
- [edit protocols l2circuit neighbor *address* interface *interface-name*]

By default, the PSN tunnel endpoint for a Layer 2 circuit is identical to the neighbor address, which is also the same as the LDP neighbor address.

The tunnel endpoints on the remote router do not need to be loopback addresses.

Example: PSN Tunnel Endpoint

The following example illustrates how you might configure a PSN tunnel endpoint:

```
[edit protocols l2circuit]
neighbor 10.255.0.6 {
  interface t1-0/2/2.0 {
    psn-tunnel-endpoint 192.0.2.2;
    virtual-circuit-id 1;
  }
  interface t1-0/2/1.0 {
    virtual-circuit-id 10;
```

```
    }
  }
```

The Layer 2 circuit configured for the **t1-0/2/2.0** interface resolves in the inet3 routing table to **192.0.2.2**. This could be either an RSVP route or a static route with an LSP next hop.

Configuring the Virtual Circuit ID

You configure a virtual circuit ID on each interface. Each virtual circuit ID uniquely identifies the Layer 2 circuit among all the Layer 2 circuits to a specific neighbor. The key to identifying a particular Layer 2 circuit on a PE router is the neighbor address and the virtual circuit ID. An LDP-FEC-to-label binding is associated with a Layer 2 circuit based on the virtual circuit ID in the FEC and the neighbor that sent this binding. The LDP-FEC-to-label binding enables the dissemination of the VPN label used for sending traffic on that Layer 2 circuit to the remote CE device.

You also configure a virtual circuit ID for each redundant pseudowire. A redundant pseudowire is identified by the backup neighbor address and the virtual circuit ID. For more information, see [“Configuring Pseudowire Redundancy on the PE Router” on page 180](#).

To configure the virtual circuit ID, include the **virtual-circuit-id** statement:

```
virtual-circuit-id identifier;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring the Interface Encapsulation Type for Layer 2 Circuits

The Layer 2 encapsulation type is carried in the LDP forwarding equivalence class (FEC). You can configure either circuit cross-connect (CCC) or translational cross-connect (TCC) encapsulation types for Layer 2 circuits. For more information, see the *Junos OS MPLS Applications Library for Routing Devices* and *Junos OS Network Interfaces Library for Routing Devices*.



NOTE: Some platform and FPC combinations can not pass TCC encapsulated ISO traffic. See *Platforms/FPCs That Cannot Forward TCC Encapsulated ISO Traffic* for details.

To configure the interface encapsulation for a Layer 2 circuit, include the **encapsulation** statement:

```
encapsulation encapsulation;
```

You can include this statement at the following hierarchy levels:

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

Configuring ATM2 IQ Interfaces for Layer 2 Circuits

You can configure Asynchronous Transfer Mode 2 (ATM2) intelligent queuing (IQ) interfaces for Layer 2 circuits by using Layer 2 circuit ATM Adaptation Layer 5 (AAL5) transport mode, Layer 2 circuit ATM cell relay mode, and the Layer 2 circuit ATM trunk mode.

The configuration statements are as follows:

- `atm-l2circuit-mode aal5`
- `atm-l2circuit-mode cell`
- `atm-l2circuit-mode trunk`

For more information about these statements, see the *Junos OS Administration Library for Routing Devices*. For more information about how to configure ATM2 IQ interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*.

The Junos OS implementation of sequence number processing for Layer 2 circuit ATM cell relay mode and Layer 2 circuit AAL5 mode differs from that described in the Internet draft draft-martini-l2circuit-encap-mpls-11.txt, *Encapsulation Methods for Transport of Layer 2 Frames over MPLS Networks* (expires August 2006).

The Junos OS implementation has the following differences:

1. A packet with a sequence number of 0 is treated as out of sequence.
2. A packet that does not have the next incremental sequence number is considered out of sequence.

When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.

Configuring Policies for Layer 2 Circuits

You can configure Junos routing policies to control the flow of packets over Layer 2 circuits. This capability allows you to provide different level of service over a set of equal-cost Layer 2 circuits. For example, you can configure a circuit for high-priority traffic, a circuit for average-priority traffic, and a circuit for low-priority traffic. By configuring Layer 2 circuit policies, you can ensure that higher-value traffic has a greater likelihood of reaching its destination.

The following sections explain how to configure Layer 2 circuit policies:

- [Configuring the Layer 2 Circuit Community on page 357](#)
- [Configuring the Policy Statement for the Layer 2 Circuit Community on page 358](#)
- [Verifying the Layer 2 Circuit Policy Configuration on page 360](#)

Configuring the Layer 2 Circuit Community

To configure a community for Layer 2 circuits, include the **community** statement.

```
community community-name {  
    members [ community-ids ];  
}
```

You can include this statement at the following hierarchy levels:

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

name identifies the community or communities.

community-ids identifies the type of community or extended community:

- A normal community uses the following community ID format:

as-number:community-value

as-number is the autonomous system (AS) number of the community member.

community-value is the identifier of the community member. It can be a number from 0 through 65,535.

- An extended community uses the following community ID format:

type:administrator:assigned-number

type is the type of target community. The target community identifies the route's destination.

administrator is either an AS number or an IP version 4 (IPv4) address prefix, depending on the type of community.

assigned-number identifies the local provider.

You also need to configure the community for the Layer 2 circuit interface; see [“Configuring a Community for the Layer 2 Circuit” on page 351](#).

Configuring the Policy Statement for the Layer 2 Circuit Community

To configure a policy to send community traffic over a specific LSP, include the **policy-statement** statement:

```
policy-statement policy-name {  
    term term-name {  
        from community community-name;  
        then {  
            install-nexthop (except | lsp lsp-name | lsp-regex lsp-regular-expression);  
            accept;  
        }  
    }  
}
```

You can include this statement at the following hierarchy levels:

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

To prevent the installation of any matching next hops, include the **install-nexthop** statement with the **except** option:

```
install-nexthop except;
```

You can include this statement at the following hierarchy levels:

- [edit policy-options policy-statement *policy-name* term *term-name* then]
- [edit logical-systems *logical-system-name* policy-options policy-statement *policy-name* term *term-name* then]

To assign traffic from a community to a specific LSP, include the **install-nexthop** statement with the **lsp** *lsp-name* option and the **accept** statement:

```
install-nexthop lsp lsp-name;  
accept;
```

You can include these statements at the following hierarchy levels:

- [edit policy-options policy-statement *policy-name* term *term-name* then]
- [edit logical-systems *logical-system-name* policy-options policy-statement *policy-name* term *term-name* then]

You can also use a regular expression to select an LSP from a set of similarly named LSPs for the **install-nexthop** statement. To configure a regular expression, include the **install-nexthop** statement with the **lsp-regex** option and the **accept** statement:

```
install-nexthop lsp-regex lsp-regular-expression;  
accept;
```

You can include these statements at the following hierarchy levels:

- [edit policy-options policy-statement *policy-name* term *term-name* then]
- [edit logical-systems *logical-system-name* policy-options policy-statement *policy-name* term *term-name* then]

Example: Configuring a Policy for a Layer 2 Circuit Community

The following example illustrates how you might configure a regular expression in a Layer 2 circuit policy. You create three LSPs to handle gold-tier traffic from a Layer 2 circuit. The LSPs are named **alpha-gold**, **beta-gold**, and **delta-gold**. You then include the **install-nexthop** statement with the **lsp-regex** option with the LSP regular expression **.*-gold** at the [edit policy-options policy-statement *policy-name* term *term-name* then] hierarchy level:

```
[edit policy-options]  
policy-statement gold-traffic {  
  term to-gold-LSPs {  
    from community gold;  
    then {  
      install-nexthop lsp-regex .*-gold;  
      accept;  
    }  
  }  
}
```

```
}  
}
```

The community **gold** Layer 2 circuits can now use any of the **-gold** LSPs. Given equal utilization across the three **-gold** LSPs, LSP selection is made at random.

You need to apply the policy to the forwarding table. To apply a policy to the forwarding table, configure the **export** statement at the **[edit routing-options forwarding-table]** hierarchy level:

```
[edit routing-options forwarding-table]  
export policy-name;
```

Verifying the Layer 2 Circuit Policy Configuration

To verify that you have configured a policy for the Layer 2 circuit, issue the **show route table mpls detail** command. It should display the community for ingress routes that corresponds to the Layer 2 circuits, as shown by the following example:

```
user@host> show route table mpls detail  
so-1/0/1.0 (1 entry, 1 announced)  
*L2VPN Preference: 7  
Next hop: via so-1/0/0.0 weight 1, selected  
Label-switched-path to-community-gold  
Label operation: Push 100000 Offset: -4  
Next hop: via so-1/0/0.0 weight 1  
Label-switched-path to-community-silver  
Label operation: Push 100000 Offset: -4  
Protocol next hop: 10.255.245.45  
Push 100000 Offset: -4  
Indirect next hop: 85333f0 314  
State: <Active Int>  
Local AS: 100  
Age: 22  
Task: Common L2 VC  
Announcement bits (2): 0-KRT 1-Common L2 VC  
AS path: I  
Communities: 100:1
```

For more information about how to configure routing policies, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*.

Configuring LDP for Layer 2 Circuits

Use LDP as the signaling protocol to advertise ingress labels to the remote PE routers. When configured, LDP examines the Layer 2 circuit configuration and initiates extended neighbor discovery for all the Layer 2 circuit neighbors (for example, remote PEs). This process is similar to how LDP works when tunneled over RSVP. You must run LDP on the **lo0.0** interface for extended neighbor discovery to function correctly.

For detailed information about how to configure LDP, see the *Junos OS MPLS Applications Library for Routing Devices*.

Configuring Class of Service with Layer 2 Circuits

- [Configuring ATM Trunking on Layer 2 Circuits on page 361](#)
- [Layer 2 Circuit Bandwidth Accounting and Call Admission Control on page 363](#)
- [Configuring Bandwidth Allocation and Call Admission Control in Layer 2 Circuits on page 365](#)

Configuring ATM Trunking on Layer 2 Circuits

You can configure Layer 2 circuits to transport ATM traffic from directly connected ATM switches across an MPLS core network. Traffic from an ATM switch is received on the local PE router. The ATM cells are given an MPLS label and then sent across the MPLS network to the remote PE router. The receiving router removes the MPLS label from the ATM cell and then forwards the cell the receiving ATM switch.



NOTE: ATM trunking on Layer 2 circuits is supported only on T Series and M320 routers and ATM2 IQ PICs.

Figure 28: ATM Trunking on Layer 2 Circuits

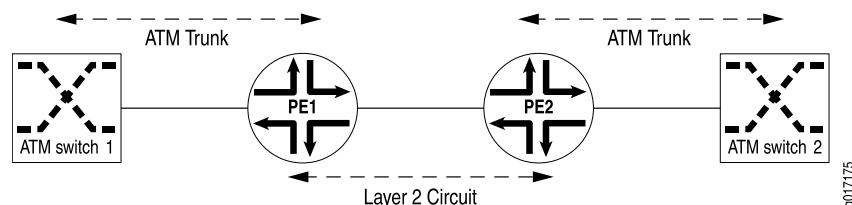


Figure 28 on page 361 illustrates how ATM switches could be linked together by a Layer 2 circuit. The PE1 Router is configured to receive ATM trunk traffic from ATM Switch 1. As each ATM cell is received on the PE1 Router, it is classified by means of the class-of-service (CoS) information in the cell header and then encapsulated as a labeled packet. The CoS information and cell loss priority (CLP) of the ATM cell are copied into the experimental (EXP) bits of the MPLS label. The labeled packet is then transported across the service provider network to the PE2 Router by means of a Layer 2 circuit.

On the PE2 Router, the label is removed and the plain ATM cell is forwarded to ATM Switch 2. The CoS and CLP are extracted from the EXP bits and are then used to select the correct output queue and determine whether the ATM cell should be dropped.

The ATM physical port on the router can support 32 logical trunks when network-to-network interface (NNI) is used and 8 logical trunks when user-to-network interface (UNI) is used. A trunk can carry traffic on 32 virtual path identifiers (VPIs), numbered 0 through 31. Each ATM trunk is associated with an MPLS label and a logical interface. On the ingress router, one or more of these trunks are mapped to a Layer 2 circuit.

The configuration for the Layer 2 circuit between PE routers is conventional. Follow the procedures outlined in this chapter for configuring the circuit. However, there is some specific configuration you need to complete for the Layer 2 circuit to carry traffic from an ATM trunk.

First, enable ATM trunking for Layer 2 circuits. To enable ATM trunking for Layer 2 circuits, specify the **trunk** option for the **atm-l2circuit-mode** statement at the **[edit chassis fpc number pic number]** hierarchy level:

```
[edit chassis fpc number pic number]
  atm-l2circuit-mode trunk (uni | nni);
```

Specify the **uni** option for UNI trunks and the **nni** option for NNI trunks. The default option is **uni**.

You also need to configure each ATM trunk for a specific logical interface. Each ATM trunk has a trunk identifier in the range from 0 to 31. This configuration step is in addition to the typical configuration steps you follow related to configuring interfaces for Layer 2 circuits, as described in [“Configuring Interfaces for Layer 2 Circuits” on page 350](#).

To associate a specific trunk identifier with a logical interface, include the **trunk-id** statement:

```
trunk-id number;
```

You can include this statement at the following hierarchy levels:

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

Since ATM trunking is supported on ATM2 IQ PICs only, the only value you can configure for the **pic-type** statement is **atm2**. If you do not configure the **pic-type** statement but you do configure the **trunk** option for the **atm-l2circuit-mode** statement (at the **[chassis fpc number pic number]** hierarchy level), the **pic-type** statement defaults to **atm2**.

Layer 2 Circuit Bandwidth Accounting and Call Admission Control

The sections that follow discuss Layer 2 circuit bandwidth accounting and call admission control (CAC):

- [Bandwidth Accounting and Call Admission Control Overview on page 363](#)
- [Selecting an LSP Based on the Bandwidth Constraint on page 363](#)
- [LSP Path Protection and CAC on page 364](#)
- [Layer 2 Circuits Trunk Mode on page 365](#)

Bandwidth Accounting and Call Admission Control Overview

Some network environments require that a certain level of service be guaranteed across the entire length of a path transiting a service provider's network. For Layer 2 circuits transiting an MPLS core network, a customer requirement might be to assure that guarantees for bandwidth and class of service (CoS) be maintained across the core network. For example, an Asynchronous Transfer Mode (ATM) circuit can provide service guarantees for each traffic class. A Layer 2 circuit configured to transport that ATM circuit across the network could be expected to provide the same service guarantees.

Providing this type of service guarantee requires the following:

- The LSPs in the MPLS core network must be able to provide service guarantees for bandwidth, rerouting, and route failures. You accomplish these guarantees by configuring multiclass LSPs. For more information about multiclass LSPs, see *Configuring Multiclass LSPs*.
- The service guarantee must be maintained across the entire length of the link as it transits the service provider's network. Different Layer 2 circuits could have different bandwidth requirements. However, many Layer 2 circuits could be transported over the same E-LSP in the MPLS core network.
- CAC ensures that the LSP has sufficient bandwidth to accommodate the Layer 2 circuit. If there is not enough bandwidth over a particular LSP, the Layer 2 circuit is prevented from using that LSP.

Selecting an LSP Based on the Bandwidth Constraint

CAC of Layer 2 circuits is based on the bandwidth constraint. You must configure this constraint for each Layer 2 circuit interface. If there is a bandwidth constraint configured for a Layer 2 circuit, CAC bases the final selection of which LSP-forwarding next hop to use on the following:

- If multiple LSPs meet the bandwidth requirements, the first LSP found that can satisfy the bandwidth requirements for the Layer 2 circuit is selected.
- If there is more than one next hop mapped to the same LSP, then all the next hops that map to that LSP and pass CAC constraints are installed. This allows the Layer 2 circuit routes to restore themselves quickly in case of failure.

- The available bandwidth on the selected LSP is decremented by the bandwidth required for each Layer 2 circuit. Similarly, when the Layer 2 circuit route is changed or deleted (for example, when the route is disassociated from that particular LSP), the bandwidth on the corresponding LSP is incremented.
- There are no priorities among different Layer 2 circuits competing for the same LSP next hop in the core network.
- When an LSP's bandwidth changes, the Layer 2 circuits using that LSP repeat the CAC process again.

If the LSP bandwidth increases, some Layer 2 circuits that were not established might now successfully resolve over the LSP. Similarly, if the bandwidth of the LSP decreases, some Layer 2 circuits that were previously up might now be declared down because of insufficient bandwidth on the LSP.

- When no LSP is found to meet the bandwidth requirements of the Layer 2 circuit, it is considered to be a CAC failure, and an error is reported.

LSP Path Protection and CAC

CAC can take into account LSPs that have been configured with an MPLS path protection feature, such as secondary paths, fast reroute, or node and link protection. CAC can consider the bandwidth available on these auxiliary links and can accept the backup connection as valid if the main connection fails. However, there are limitations on how the path protection feature must be configured to prevent CAC from taking down the Layer 2 circuit when the LSP it is using is switched to a backup route.

For more information about MPLS path protection features, see the *MPLS and Traffic Protection*.

The sections that follow discuss the path protection features that can be used in conjunction with CAC and how they must be configured:

- [Secondary Paths and CAC on page 364](#)
- [Fast Reroute and CAC on page 365](#)
- [Link and Node Protection and CAC on page 365](#)

Secondary Paths and CAC

The following describes the ways in which secondary paths would interact with Layer 2 circuit CAC:

- If an LSP is configured with both primary and secondary paths, if the paths have the same bandwidth, and if this bandwidth is enough to accommodate the Layer 2 circuit, the Layer 2 circuit route installs both next hops in the forwarding table.

CAC allows the Layer 2 circuit to be switched to the secondary path if the primary path fails.

- If the LSP has primary and secondary paths configured with different bandwidths, each path must run through CAC independently. If the active path for that LSP passes CAC constraints successfully, then that next hop is installed and the corresponding LSP is

selected to transport the Layer 2 circuit traffic. The LSP's secondary paths are then checked for CAC, and installed if there is sufficient bandwidth.

However, if the active path for the LSP fails to meet the CAC constraints, then that LSP is not selected and the system looks for a different LSP to transport the Layer 2 circuit.

For example, an LSP has an active primary path with 30 megabits of bandwidth and a secondary path with 10 megabits of bandwidth. The Layer 2 circuit requires 15 megabits of bandwidth. The secondary path fails CAC, and only the next hop corresponding to the primary path is installed for the Layer 2 circuit route. The path protection originally provided by the secondary path is no longer available.

Fast Reroute and CAC

No CAC is done for fast reroute detours. However, as long as the protected path satisfies the CAC bandwidth constraints, the detour next hop is also selected and installed.

Link and Node Protection and CAC

You can configure CAC on Layer 2 circuit-based LSPs with bandwidth constraints and also enable link and node protection. However, if the primary LSP fails, CAC might not be applied to the bypass LSP, meaning the bypass LSP might not meet the bandwidth constraint for the Layer 2 circuit. To minimize the risk of losing traffic, the Layer 2 circuit continues to use the non-CAC bypass LSP while an attempt is made to establish a new Layer 2 circuit route over an LSP that does support CAC.

Layer 2 Circuits Trunk Mode

Using Layer 2 circuit trunk mode, you can configure Layer 2 circuits to carry ATM trunks, providing a way to link ATM switches over an MPLS core network.

Layer 2 circuit trunk mode allows you to configure the following CoS features:

- CoS queues in Layer 2 circuit trunk mode—For ATM2 IQ interfaces, you can configure ATM CoS queues for Layer 2 circuit trunk mode.
- Layer 2 circuit trunk mode scheduling—For ATM2 IQ interfaces configured to use Layer 2 circuit trunk mode, you can share a scheduler among 32 trunks on an ATM port.
- Two early packet discard (EPD) thresholds per queue—For ATM2 IQ interfaces configured to use Layer 2 circuit trunk mode, you can set two EPD thresholds that depend on the packet-loss priorities (PLPs) of the packets.

For a detailed overview and configuration documentation, see the *ATM Interfaces Feature Guide for Routing Devices Class of Service Feature Guide for Routing Devices*.

Related Documentation

- *MPLS and Traffic Protection*

Configuring Bandwidth Allocation and Call Admission Control in Layer 2 Circuits

You can configure bandwidth allocation and call admission control (CAC) on Layer 2 circuits. This feature is available for RSVP-signaled LSPs traversing an MPLS network.

When you enable bandwidth allocation on a Layer 2 circuit, attempts to establish an RSVP-signaled LSP are preceded by a check of the available bandwidth on the network. This check is the CAC. The available bandwidth is compared to the bandwidth requested by the LSP. If there is insufficient bandwidth, the Layer 2 circuit is not established and an error message is generated. To apply CAC to a Layer 2 circuit, a bandwidth constraint must be configured.

You can specify the bandwidth for a Layer 2 circuit without configuring a bandwidth for each class type (queue). To specify the bandwidth allocation for a Layer 2 circuit, include the **bandwidth** statement:

```
bandwidth bandwidth;
```

Specify the bandwidth in bits per second.

You can include this statement at the following hierarchy levels:

- [edit protocols l2circuit neighbor *address* interface *interface-name*]
- [edit logical-systems *logical-system-name* protocols l2circuit neighbor *address* interface *interface-name*]

Alternatively, you can configure the bandwidth for each class type on a Layer 2 circuit. If you use this type of configuration, you cannot simultaneously configure the nonclass type of bandwidth configuration for the Layer 2 circuit (the commit operation fails).

To configure the bandwidth for each class type on an Layer 2 circuit, include the **bandwidth** statement:

```
bandwidth {  
  ct0 bandwidth;  
  ct1 bandwidth;  
  ct2 bandwidth;  
  ct3 bandwidth;  
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols l2circuit neighbor *address* interface *interface-name*]
- [edit logical-systems *logical-system-name* protocols l2circuit neighbor *address* interface *interface-name*]

Specify the bandwidth for each class type in bits per second. It is not necessary to specify a bandwidth for all four class types.

Configuring Pseudowire Redundancy for Layer 2 Circuits

- [Understanding Pseudowire Redundancy Mobile Backhaul Scenarios on page 367](#)
- [Example: Configuring Pseudowire Redundancy in a Mobile Backhaul Scenario on page 371](#)

Understanding Pseudowire Redundancy Mobile Backhaul Scenarios

With the rising demand for mobile broadband services, telecommunication providers are seeing a sharp increase in bandwidth requirements. To keep pace with demand, operators are deploying packet-based backhaul networks that offer increased capacity at a lower cost, while providing the necessary service reliability and quality of experience that users expect.

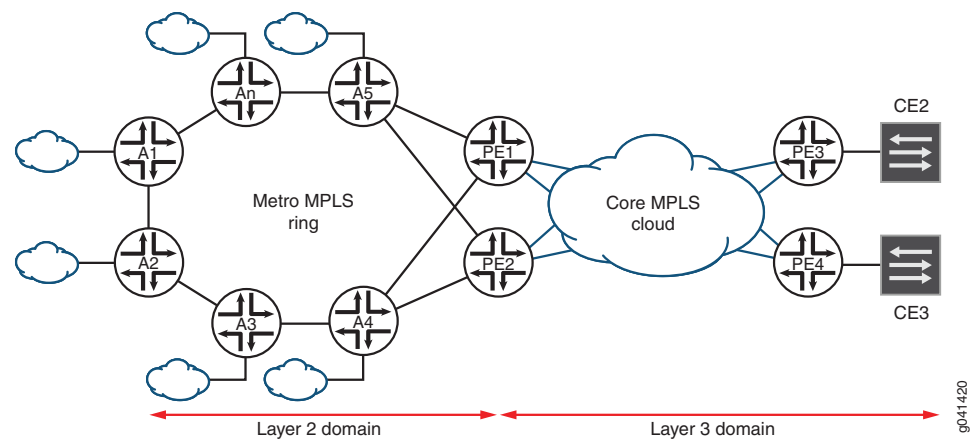
Most of the legacy backhaul infrastructure has been traditionally built over PDH microwave, TDM T1/E1, or ATM-over-DSL links. Service providers have traditionally added subsequent TDM links to their base stations when needed to deal with bandwidth constraint scenarios. This expansion model has proven to be inefficient for the unprecedented traffic demands required by 3G and Long Term Evolution (LTE) services. As a direct consequence, operators are gradually migrating to an Ethernet-based higher capacity infrastructure in the backhaul portion of 3G and LTE topologies. Modern base stations now provide Ethernet backhaul connectivity, allowing pseudowire technologies to transport end-user content to the desired destination. As part of this Ethernet transition, service providers are increasingly demanding better resiliency mechanisms to cover the existence gap with those features provided by previous legacy technologies. With that goal in mind, Junos OS provides efficient pseudowire redundancy capabilities to those topologies where Layer 2 and Layer 3 segments are interconnected.

- [Sample Topology on page 367](#)
- [Benefits of Pseudowire Redundancy Mobile Backhaul on page 368](#)
- [Layer 2 Virtual Circuit Status TLV Extension on page 368](#)
- [How It Works on page 369](#)

Sample Topology

[Figure 29 on page 368](#) shows a sample topology.

Figure 29: Pseudowire Redundancy Mobile Backhaul Sample Topology



Benefits of Pseudowire Redundancy Mobile Backhaul

Junos OS pseudowire redundancy capabilities are as follows:

- Redundant loop-free paths to interconnect Layer 2 and Layer 3 domains.
- Layer 2 and Layer 3 domains are synchronized with regard to the elected data path.
- Traffic disruption is minimal for the following possible scenarios:
 - Access link failures
 - Node failures
 - Control-plane failures
- Traffic interruption is minimal after the failure's restoration is completed.

Layer 2 Virtual Circuit Status TLV Extension

The pseudowire status TLV is used to communicate the status of a pseudowire between PE routers. To avoid potential primary-path discrepancies, there must be a mechanism that allows all network elements to be synchronized with respect to the primary path over which traffic needs to be sent. With this goal in mind, the status TLV is extended to address this requirement.

By having the active and standby states being defined by the access routers, Junos OS mitigates potential primary path collisions, as there is a unique network element dictating the preferable forwarding path to be elected. As an added value, this allows network operators to switch forwarding paths on demand, which is quite useful for troubleshooting and network maintenance purposes.

The active and standby states are communicated to the aggregation routers by making use of an additional pseudowire state flag.

Table 12 on page 369 includes a list of the pseudowire state flags.

Table 12: Pseudowire Status Code for the Pseudowire Status TLV

Flag	Code
L2CKT_PW_STATUS_PW_FWD	0x00000000
L2CKT_PW_STATUS_PW_NOT_FWD	0x00000001
L2CKT_PW_STATUS_AC_RX_FAULT	0x00000002
L2CKT_PW_STATUS_AC_TX_FAULT	0x00000004
L2CKT_PW_STATUS_PSN_RX_FAULT	0x00000008
L2CKT_PW_STATUS_PSN_TX_FAULT	0x00000010
L2CKT_PW_STATUS_PW_FWD_STDBY	0x00000020
	Indicates the standby state.
L2CKT_PW_STATUS_SWITCH_OVER	0x00000040

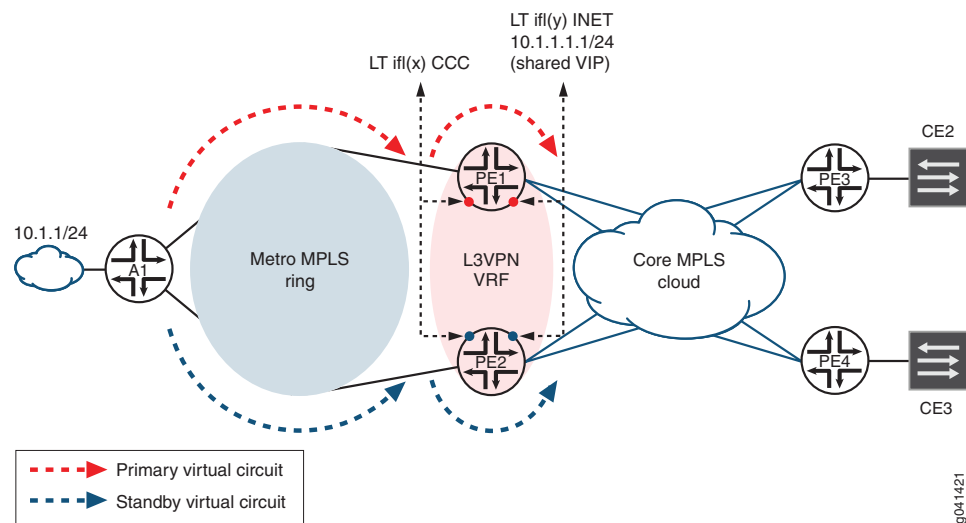
In multichassis LAG (MC-LAG)-based scenarios, this same PW_FWD_STDBY flag is used to advertise to remote PE devices which attachment circuit (AC) is being used as the active one. Upon arrival of this flag, the receiving PE device drops any pseudowire built toward the router originating this state. As we can see, this behavior denotes a slightly different semantic for the PW_FWD_STDBY flag. As a consequence, you can configure the **hot-standby-vc-on** statement to control whether the pseudowire must be constructed upon arrival of the PW_FWD_STDBY flag (in the hot-standby pseudowire scenario), or simply destroy it (in the MC-LAG scenario).

How It Works

The solution uses logical tunnel (lt-) paired interfaces for stitching the Layer 2 and Layer 3 domains.

[Figure 30 on page 370](#) shows a diagram depicting how pseudowire redundancy in a mobile backhaul scenario works.

Figure 30: Pseudowire Redundancy Mobile Backhaul Solution



A Layer 2 pseudowire terminates on one of the logical tunnel interfaces (x), defined with the circuit cross-connect (CCC) address family configured. A Layer 3 VPN (RFC 2547) terminates the second logical tunnel interface (y), defined with the IPv4 (inet) address family. Logical tunnel interface (x) and (y) are paired. Layer 2 pseudowires established between each access router and its corresponding aggregation PE devices terminate on the logical tunnel interface defined within each PE device. This logical tunnel interface is used to establish a Layer 2 virtual circuit (VC) toward the remote end. In consequence, the CCC address family needs to be configured on it. The same applies to the remote end, where an equivalent interface needs to be defined with CCC capabilities.

This CCC logical tunnel interface created in the aggregation PE devices is paired with a second logical tunnel interface on which the INET address family is enabled. This second logical tunnel interface is configured within the context of an RFC 2547 Layer 3 VPN.

Within the scope of this document, we refer to the CCC and INET logical tunnel interfaces as LT(x) and LT(y), respectively.

The Junos OS routing protocol process (rpd) enables the stitching required to interconnect the Layer 2 VC ending in LT(x) and the associated LT(y).

In the aggregation PE routers, the routing process builds a pseudowire toward access routers, and this happens regardless of the active or standby state of the pseudowire. The same occurs in access routers, where the control and forwarding state is preestablished in both the Routing Engine and in the Packet Forwarding Engine to mitigate traffic disruption during convergence periods.

An attachment circuit (AC) is a physical or virtual circuit (VC) that attaches a CE device to a PE device. Local preference is used to provide better information than the multiple exit discriminator (MED) value provides for a packet's path selection. You can configure the local preference attribute so that it has a higher value for prefixes received from a router that provides a desired path than prefixes received from a router that provides a less desirable path. The higher the value, the more preferred the route. The local

preference attribute is the metric most often used in practice to express preferences for one set of paths over another.

If the Layer 2 circuit is primary, the corresponding PE device advertises the AC's subnet with the higher local preference. All aggregation PE devices initially advertise the AC's subnet with the same local preference. You can configure a routing policy to allow a higher local preference value to be advertised if the Layer 2 VC is active.

If a pseudowire is down, LT(x) is tagged with the CCC_Down flag. When this happens, the corresponding PE device withdraws the AC subnet that was initially advertised. The LT(y) address is shared between the aggregation PE devices as a virtual instance port (VIP). No VRRP hello messages are exchanged. Both PE devices assume mastership.

Both primary and standby Layer 2 VCs are kept open to reduce traffic disruption in backup-to-primary transitions. The **hot-standby-vc-on** configuration statement allows manual activation.

Resiliency in the Layer 2 domain is provided through plain pseudowire redundancy for back-to-back connections. For other topologies, pseudowire virtual circuit connectivity verification (VCCV) is used.

Resiliency in the Layer 3 domain is provided by MPLS fast reroute and end-to-end service restoration. A restoration timer prevents having VCs in the secondary path from being switched back to the primary path immediately after the master PE device is restored.

Access routers can indicate to the aggregation routers which Layer 2 VC is considered to be active. Upon arrival at LT(x) of a status TLV message communicating a standby state, the routing process decreases the BGP's local preference value of the direct subnet represented by the LT(y) IPv4 address. At this point, BGP proceeds to advertise this local preference change to the rest of the members within the Layer 3 domain, which will then reelect the designated forwarder PE device by relying on BGP's path selection mechanisms.

A similar behavior occurs upon arrival of a status TLV message indicating a Layer 2 VC active state. In this case, the receiving PE device changes the local preference corresponding to the LT(y)'s subnet. The value to be used to either decrease or increase the subnet's local preference value is manually configured using a policy.

**Related
Documentation**

- [Example: Configuring Pseudowire Redundancy in a Mobile Backhaul Scenario on page 371](#)

Example: Configuring Pseudowire Redundancy in a Mobile Backhaul Scenario

This example shows how to configure pseudowire redundancy where Layer 2 and Layer 3 segments are interconnected in a mobile backhaul scenario.

- [Requirements on page 372](#)
- [Overview on page 372](#)
- [Configuration on page 373](#)
- [Verification on page 390](#)

Requirements

This example can be configured using the following hardware and software components:

- Junos OS Release 13.2 or later
- MX Series 3D Universal Edge Routers or M Series Multiservice Edge Routers for the Provider Edge (PE) Routers
- PTX Series Packet Transport Routers acting as transit label-switched routers
- T Series Core Routers for the Core Routers



NOTE: The PE routers could also be T Series Core Routers but that is not typical. Depending on your scaling requirements, the core routers could also be MX Series 3D Universal Edge Routers or M Series Multiservice Edge Routers. The Customer Edge (CE) devices could be other routers or switches from Juniper Networks or another vendor.

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

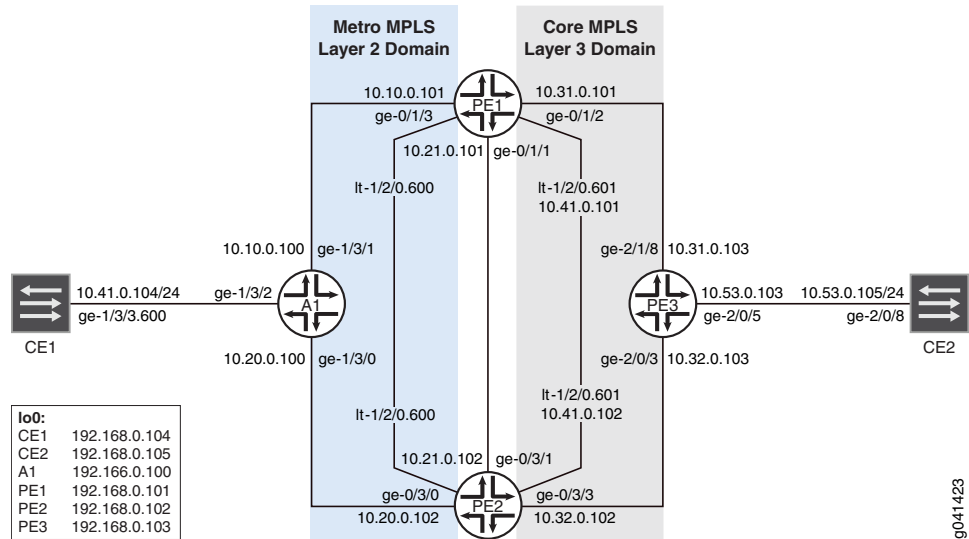
Overview

Device CE1 is a simple edge router with an IPv4 interface and a static route pointing to the PE devices. Device A1 establishes two virtual circuits (VCs) toward Device PE1 and Device PE2 by making use of the **hot-standby** statement. Device PE1 and Device PE2 terminate these VCs and enforce a policy condition over the logical tunnel IPv4 subnet. Device PE3 performs as a Layer 3 VPN provider edge device by having an IPv4 interface in a Layer 3 VPN shared with Device PE1 and Device PE2.

[“CLI Quick Configuration” on page 373](#) shows the configuration for all of the devices in [Figure 31 on page 373](#).

The section [“Step-by-Step Procedure” on page 378](#) describes the steps on Device A1 and Device PE1.

Figure 31: Pseudowire Redundancy in a Mobile Backhaul Example Topology



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-1/3/3 vlan-tagging
set interfaces ge-1/3/3 unit 600 vlan-id 600
set interfaces ge-1/3/3 unit 600 family inet address 10.41.0.104/24
set interfaces lo0 unit 0 family inet address 192.168.0.104/32 primary
set interfaces lo0 unit 0 family inet address 192.168.0.104/32 primary
set protocols ospf area 0.0.0.0 interface ge-1/3/3.600
set protocols ospf area 0.0.0.0 interface lo0.0
set routing-options static route 192.168.0.0/8 next-hop 10.41.0.1
set routing-options static route 10.53.0.0/16 next-hop 10.41.0.1
set routing-options router-id 192.168.0.104
```

Device A1

```
set interfaces ge-1/3/0 unit 0 family inet address 10.20.0.100/24
set interfaces ge-1/3/0 unit 0 family iso
set interfaces ge-1/3/0 unit 0 family mpls
set interfaces ge-1/3/1 unit 0 family inet address 10.10.0.100/24
set interfaces ge-1/3/1 unit 0 family iso
set interfaces ge-1/3/1 unit 0 family mpls
set interfaces ge-1/3/2 vlan-tagging
set interfaces ge-1/3/2 encapsulation vlan-ccc
set interfaces ge-1/3/2 unit 600 encapsulation vlan-ccc
set interfaces ge-1/3/2 unit 600 vlan-id 600
set interfaces ge-1/3/2 unit 600 family ccc
set interfaces lo0 unit 0 family inet address 192.168.0.100/32 primary
set interfaces lo0 unit 0 family iso address 49.0002.0192.0168.0100.00
set routing-options router-id 192.168.0.100
set routing-options autonomous-system 64510
set routing-options forwarding-table export pplib
```

```

set protocols rsvp interface ge-1/3/0.0
set protocols rsvp interface ge-1/3/1.0
set protocols rsvp interface lo0.0
set protocols mpls interface ge-1/3/0.0
set protocols mpls interface ge-1/3/1.0
set protocols isis interface ge-1/3/0.0
set protocols isis interface ge-1/3/1.0
set protocols isis interface lo0.0
set protocols ldp interface ge-1/3/0.0
set protocols ldp interface ge-1/3/1.0
set protocols ldp interface lo0.0
set protocols l2circuit neighbor 192.168.0.101 interface ge-1/3/2.600 virtual-circuit-id 1
set protocols l2circuit neighbor 192.168.0.101 interface ge-1/3/2.600 pseudowire-status-tlv
set protocols l2circuit neighbor 192.168.0.101 interface ge-1/3/2.600 revert-time 10
    maximum 60
set protocols l2circuit neighbor 192.168.0.101 interface ge-1/3/2.600 backup-neighbor
    192.168.0.102 virtual-circuit-id 2
set protocols l2circuit neighbor 192.168.0.101 interface ge-1/3/2.600 backup-neighbor
    192.168.0.102 hot-standby
set policy-options policy-statement pplb then load-balance per-packet

```

Device PE1

```

set interfaces ge-0/1/1 unit 0 family inet address 10.21.0.101/24
set interfaces ge-0/1/1 unit 0 family iso
set interfaces ge-0/1/1 unit 0 family mpls
set interfaces ge-0/1/2 unit 0 family inet address 10.31.0.101/24
set interfaces ge-0/1/2 unit 0 family iso
set interfaces ge-0/1/2 unit 0 family mpls
set interfaces ge-0/1/3 unit 0 family inet address 10.10.0.101/24
set interfaces ge-0/1/3 unit 0 family iso
set interfaces ge-0/1/3 unit 0 family mpls
set interfaces lt-1/2/0 unit 600 encapsulation vlan-ccc
set interfaces lt-1/2/0 unit 600 vlan-id 600
set interfaces lt-1/2/0 unit 600 peer-unit 601
set interfaces lt-1/2/0 unit 601 encapsulation vlan
set interfaces lt-1/2/0 unit 601 vlan-id 600
set interfaces lt-1/2/0 unit 601 peer-unit 600
set interfaces lt-1/2/0 unit 601 family inet filter input icmp_inet
set interfaces lt-1/2/0 unit 601 family inet filter output icmp_inet
set interfaces lt-1/2/0 unit 601 family inet address 10.41.0.101/24 vrrp-group 0
    virtual-address 10.41.0.1
set interfaces lt-1/2/0 unit 601 family inet address 10.41.0.101/24 vrrp-group 0 accept-data
set interfaces lo0 unit 0 family inet address 192.168.0.101/32 primary
set interfaces lo0 unit 0 family iso address 49.0002.0192.0168.0003.00
set interfaces lo0 unit 1 family inet address 192.168.1.101/32
set routing-options router-id 192.168.0.101
set routing-options autonomous-system 64511
set protocols rsvp interface ge-0/1/1.0
set protocols rsvp interface ge-0/1/2.0
set protocols rsvp interface ge-0/1/3.0
set protocols rsvp interface lo0.0
set protocols mpls label-switched-path to_PE3 to 192.168.0.103
set protocols mpls label-switched-path to_PE2 to 192.168.0.102
set protocols mpls interface ge-0/1/1.0
set protocols mpls interface ge-0/1/2.0
set protocols mpls interface ge-0/1/3.0
set protocols bgp local-address 192.168.0.101

```

```

set protocols bgp group ibgp family inet-vpn any
set protocols bgp group ibgp peer-as 64511
set protocols bgp group ibgp neighbor 192.168.0.102
set protocols bgp group ibgp neighbor 192.168.0.103
set protocols isis interface ge-0/1/1.0
set protocols isis interface ge-0/1/2.0
set protocols isis interface ge-0/1/3.0
set protocols isis interface lo0.0
set protocols ldp interface ge-0/1/1.0
set protocols ldp interface ge-0/1/2.0
set protocols ldp interface ge-0/1/3.0
set protocols ldp interface lo0.0
set protocols l2circuit neighbor 192.168.0.100 interface lt-1/2/0.600 virtual-circuit-id 1
set protocols l2circuit neighbor 192.168.0.100 interface lt-1/2/0.600 pseudowire-status-tlv
    hot-standby-vc-on
set policy-options policy-statement l3vpn_export term primary from condition primary
set policy-options policy-statement l3vpn_export term primary then local-preference
    add 300
set policy-options policy-statement l3vpn_export term primary then community set l3vpn
set policy-options policy-statement l3vpn_export term primary then accept
set policy-options policy-statement l3vpn_export term standby from condition standby
set policy-options policy-statement l3vpn_export term standby then local-preference
    add 30
set policy-options policy-statement l3vpn_export term standby then community set l3vpn
set policy-options policy-statement l3vpn_export term standby then accept
set policy-options policy-statement l3vpn_export term default then community set l3vpn
set policy-options policy-statement l3vpn_export term default then accept
set policy-options policy-statement l3vpn_import term 1 from community l3vpn
set policy-options policy-statement l3vpn_import term 1 then accept
set policy-options policy-statement l3vpn_import term default then reject
set policy-options policy-statement ospf_export term 0 from community l3vpn
set policy-options policy-statement ospf_export term 0 then accept
set policy-options community l3vpn members target:64511:600
set policy-options condition primary if-route-exists address-family ccc lt-1/2/0.600
set policy-options condition primary if-route-exists address-family ccc table mpls.0
set policy-options condition primary if-route-exists address-family ccc peer-unit 601
set policy-options condition standby if-route-exists address-family ccc lt-1/2/0.600
set policy-options condition standby if-route-exists address-family ccc table mpls.0
set policy-options condition standby if-route-exists address-family ccc standby
set policy-options condition standby if-route-exists address-family ccc peer-unit 601
set firewall family inet filter icmp_inet interface-specific
set firewall family inet filter icmp_inet term 0 from source-address 10.41.0.101/32 except
set firewall family inet filter icmp_inet term 0 from source-address 10.0.0.0/8
set firewall family inet filter icmp_inet term 0 from protocol icmp
set firewall family inet filter icmp_inet term 0 then count icmp_inet
set firewall family inet filter icmp_inet term 0 then log
set firewall family inet filter icmp_inet term 0 then accept
set firewall family inet filter icmp_inet term 1 then accept
set routing-instances l3vpn instance-type vrf
set routing-instances l3vpn interface lt-1/2/0.601
set routing-instances l3vpn interface lo0.1
set routing-instances l3vpn route-distinguisher 192.168.1.101:64511
set routing-instances l3vpn vrf-import l3vpn_import
set routing-instances l3vpn vrf-export l3vpn_export
set routing-instances l3vpn vrf-table-label
set routing-instances l3vpn protocols ospf export ospf_export

```

```

set routing-instances l3vpn protocols ospf area 0.0.0.0 lt-1/2/0.601
set routing-instances l3vpn protocols ospf area 0.0.0.0 lo0.1

```

```

Device PE2
set interfaces ge-0/3/0 unit 0 family inet address 10.20.0.102/24
set interfaces ge-0/3/0 unit 0 family iso
set interfaces ge-0/3/0 unit 0 family mpls
set interfaces ge-0/3/1 unit 0 family inet address 10.21.0.102/24
set interfaces ge-0/3/1 unit 0 family iso
set interfaces ge-0/3/1 unit 0 family mpls
set interfaces ge-0/3/3 unit 0 family inet address 10.32.0.102/24
set interfaces ge-0/3/3 unit 0 family iso
set interfaces ge-0/3/3 unit 0 family mpls
set interfaces lt-1/2/0 unit 600 encapsulation vlan-ccc
set interfaces lt-1/2/0 unit 600 vlan-id 600
set interfaces lt-1/2/0 unit 600 peer-unit 601
set interfaces lt-1/2/0 unit 601 encapsulation vlan
set interfaces lt-1/2/0 unit 601 vlan-id 600
set interfaces lt-1/2/0 unit 601 peer-unit 600
set interfaces lt-1/2/0 unit 601 family inet filter input icmp_inet
set interfaces lt-1/2/0 unit 601 family inet filter output icmp_inet
set interfaces lt-1/2/0 unit 601 family inet address 10.41.0.102/24 vrrp-group 0
    virtual-address 10.41.0.1
set interfaces lt-1/2/0 unit 601 family inet address 10.41.0.102/24 vrrp-group 0 accept-data
set interfaces lo0 unit 0 family inet address 192.168.0.102/32 primary
set interfaces lo0 unit 0 family iso address 49.0002.0192.0168.0102.00
set interfaces lo0 unit 1 family inet address 192.168.1.102/32
set routing-options router-id 192.168.0.102
set routing-options autonomous-system 64511
set protocols rsvp interface ge-0/3/0.0
set protocols rsvp interface ge-0/3/1.0
set protocols rsvp interface ge-0/3/3.0
set protocols rsvp interface lo0.0
set protocols mpls label-switched-path to_PE1 to 192.168.0.101
set protocols mpls label-switched-path to_PE3 to 192.168.0.103
set protocols mpls interface ge-0/3/0.0
set protocols mpls interface ge-0/3/1.0
set protocols mpls interface ge-0/3/3.0
set protocols bgp local-address 192.168.0.102
set protocols bgp group ibgp family inet-vpn any
set protocols bgp group ibgp peer-as 64511
set protocols bgp group ibgp neighbor 192.168.0.101
set protocols bgp group ibgp neighbor 192.168.0.103
set protocols isis interface ge-0/3/0.0
set protocols isis interface ge-0/3/1.0
set protocols isis interface ge-0/3/3.0
set protocols isis interface lo0.0
set protocols ldp interface ge-0/3/0.0
set protocols ldp interface ge-0/3/1.0
set protocols ldp interface ge-0/3/3.0
set protocols ldp interface lo0.0
set protocols l2circuit neighbor 192.168.0.100 interface lt-1/2/0.600 virtual-circuit-id 2
set protocols l2circuit neighbor 192.168.0.100 interface lt-1/2/0.600 pseudowire-status-tlv
    hot-standby-vc-on
set policy-options policy-statement l3vpn_export term primary from condition primary
set policy-options policy-statement l3vpn_export term primary then local-preference
    add 300

```

```

set policy-options policy-statement l3vpn_export term primary then community set l3vpn
set policy-options policy-statement l3vpn_export term primary then accept
set policy-options policy-statement l3vpn_export term standby from condition standby
set policy-options policy-statement l3vpn_export term standby then local-preference
  add 30
set policy-options policy-statement l3vpn_export term standby then community set l3vpn
set policy-options policy-statement l3vpn_export term standby then accept
set policy-options policy-statement l3vpn_export term default then community set l3vpn
set policy-options policy-statement l3vpn_export term default then accept
set policy-options policy-statement l3vpn_import term 1 from community l3vpn
set policy-options policy-statement l3vpn_import term 1 then accept
set policy-options policy-statement l3vpn_import term default then reject
set policy-options policy-statement ospf_export term 0 from community l3vpn
set policy-options policy-statement ospf_export term 0 then accept
set policy-options community l3vpn members target:64511:600
set policy-options condition primary if-route-exists address-family ccc lt-1/2/0.600
set policy-options condition primary if-route-exists address-family ccc table mpls.0
set policy-options condition primary if-route-exists address-family ccc peer-unit 601
set policy-options condition standby if-route-exists address-family ccc lt-1/2/0.600
set policy-options condition standby if-route-exists address-family ccc table mpls.0
set policy-options condition standby if-route-exists address-family ccc standby
set policy-options condition standby if-route-exists address-family ccc peer-unit 601
set firewall family inet filter icmp_inet interface-specific
set firewall family inet filter icmp_inet term 0 from source-address 10.41.0.102/32 except
set firewall family inet filter icmp_inet term 0 from source-address 10.0.0.0/8
set firewall family inet filter icmp_inet term 0 from protocol icmp
set firewall family inet filter icmp_inet term 0 then count icmp_inet
set firewall family inet filter icmp_inet term 0 then log
set firewall family inet filter icmp_inet term 0 then accept
set firewall family inet filter icmp_inet term 1 then accept
set routing-instances l3vpn instance-type vrf
set routing-instances l3vpn interface lt-1/2/0.601
set routing-instances l3vpn interface lo0.1
set routing-instances l3vpn route-distinguisher 192.168.1.102:64511
set routing-instances l3vpn vrf-import l3vpn_import
set routing-instances l3vpn vrf-export l3vpn_export
set routing-instances l3vpn vrf-table-label
set routing-instances l3vpn protocols ospf export ospf_export
set routing-instances l3vpn protocols ospf area 0.0.0.0 interface lt-1/2/0.601
set routing-instances l3vpn protocols ospf area 0.0.0.0 interface lo0.1

```

Device PE3

```

set interfaces ge-2/0/3 unit 0 family inet address 10.32.0.103/24
set interfaces ge-2/0/3 unit 0 family iso
set interfaces ge-2/0/3 unit 0 family mpls
set interfaces ge-2/0/5 unit 0 family inet address 10.53.0.103/24
set interfaces ge-2/0/5 unit 0 family mpls
set interfaces ge-2/1/8 unit 0 family inet address 10.31.0.103/24
set interfaces ge-2/1/8 unit 0 family iso
set interfaces ge-2/1/8 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 192.168.0.103/32 primary
set interfaces lo0 unit 0 family iso address 49.0002.0192.0168.0103.00
set interfaces lo0 unit 1 family inet address 192.168.1.103/32
set routing-options router-id 192.168.0.103
set routing-options autonomous-system 64511
set protocols rsvp interface ge-2/0/3.0
set protocols rsvp interface ge-2/1/8.0

```

```

set protocols rsvp interface lo0.0
set protocols mpls label-switched-path to_PE1 to 192.168.0.101
set protocols mpls label-switched-path to_PE2 to 192.168.0.102
set protocols mpls interface ge-2/0/3.0
set protocols mpls interface ge-2/1/8.0
set protocols bgp local-address 192.168.0.103
set protocols bgp group ibgp family inet-vpn any
set protocols bgp group ibgp peer-as 64511
set protocols bgp group ibgp neighbor 192.168.0.101
set protocols bgp group ibgp neighbor 192.168.0.102
set protocols isis interface ge-2/0/3.0
set protocols isis interface ge-2/1/8.0
set protocols isis interface lo0.0
set protocols ldp interface ge-2/0/3.0
set protocols ldp interface ge-2/1/8.0
set protocols ldp interface lo0.0
set policy-options policy-statement l3vpn_ospf_export term 0 from protocol direct
set policy-options policy-statement l3vpn_ospf_export term 0 then accept
set policy-options policy-statement l3vpn_ospf_import term 0 from protocol bgp
set policy-options policy-statement l3vpn_ospf_import term 0 from community l3vpn
set policy-options policy-statement l3vpn_ospf_import term 0 then accept
set policy-options policy-statement ospf_export term 0 from community l3vpn
set policy-options policy-statement ospf_export term 0 then accept
set policy-options community l3vpn members target:64511:600
set routing-instances l3vpn instance-type vrf
set routing-instances l3vpn interface ge-2/0/5.0
set routing-instances l3vpn interface lo0.1
set routing-instances l3vpn route-distinguisher 192.168.0.103:64511
set routing-instances l3vpn vrf-target target:64511:600
set routing-instances l3vpn vrf-table-label
set routing-instances l3vpn protocols ospf export ospf_export
set routing-instances l3vpn protocols ospf area 0.0.0.0 interface ge-2/0/5.0
set routing-instances l3vpn protocols ospf area 0.0.0.0 interface lo0.1

```

Device CE2

```

set interfaces ge-2/0/8 unit 0 family inet address 10.53.0.105/24
set interfaces lo0 unit 0 family inet address 192.168.0.105/32 primary
set protocols ospf area 0.0.0.0 interface ge-2/0/8.0
set protocols ospf area 0.0.0.0 interface lo0.0
set routing-options router-id 192.168.0.105

```

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 Device A1:

1. Configure the interfaces.

Enable MPLS on the core-facing interfaces. The ISO address family is also enabled, because IS-IS is used as the interior gateway protocol (IGP) in the provider network.

On the customer-facing interface, you do not need to enable MPLS. On this interface, enable CCC encapsulation and address family CCC.

```

[edit interfaces]
user@A1# set ge-1/3/0 unit 0 family inet address 10.20.0.100/24

```

```
user@A1# set ge-1/3/0 unit 0 family iso
user@A1# set ge-1/3/0 unit 0 family mpls
```

```
user@A1# set ge-1/3/1 unit 0 family inet address 10.10.0.100/24
user@A1# set ge-1/3/1 unit 0 family iso
user@A1# set ge-1/3/1 unit 0 family mpls
```

```
user@A1# set ge-1/3/2 vlan-tagging
user@A1# set ge-1/3/2 encapsulation vlan-ccc
user@A1# set ge-1/3/2 unit 600 encapsulation vlan-ccc
user@A1# set ge-1/3/2 unit 600 vlan-id 600
user@A1# set ge-1/3/2 unit 600 family ccc
```

```
user@A1# set lo0 unit 0 family inet address 192.168.0.100/32 primary
user@A1# set lo0 unit 0 family iso address 49.0002.0192.0168.0100.00
```

2. Configure the RSVP on the core-facing interfaces and on the loopback interface.

RSVP is used in the Layer 3 domain.

```
[edit protocols rsvp]
user@A1# set interface ge-1/3/0.0
user@A1# set interface ge-1/3/1.0
user@A1# set interface lo0.0
```

3. Configure LDP on the core-facing interfaces and on the loopback interface.

LDP is used in Layer 2 domain.

```
[edit protocols ldp]
user@A1# set interface ge-1/3/0.0
user@A1# set interface ge-1/3/1.0
user@A1# set interface lo0.0
```

4. Configure MPLS on the core-facing interfaces.

```
[edit protocols mpls]
user@A1# set interface ge-1/3/0.0
user@A1# set interface ge-1/3/1.0
```

5. Configure an interior gateway protocol, such as IS-IS or OSPF, on the core-facing interfaces and on the loopback interface.

```
[edit protocols isis]
user@A1# set interface ge-1/3/0.0
user@A1# set interface ge-1/3/1.0
user@A1# set interface lo0.0
```

6. On the interface that faces the customer edge, configure the Layer 2 circuit.

Configure the **hot-standby** statement on those routers with both active and standby virtual circuits (VCs) (Device A1 in our topology). You must include the **pseudowire-status-tlv** statement on access routers. Without the status TLV signaling, the standby flag cannot be advertised to remote provider edge (PE) devices.

The **revert-time** statement and the **maximum** option should also be configured on access routers. Without the **revert-time** statement, traffic of all the VCs will not be transitioned to the primary path upon completion of the restoration. If a **revert-time**

delay is defined but a **maximum** delay is not, then VCs are restored immediately upon the revert timer's expiration. The maximum option allows the VCs to be restored in a scattered fashion rather than all at once.

```
[edit protocols l2circuit neighbor 192.168.0.101 interface ge-1/3/2.600]
user@A1# set virtual-circuit-id 1
user@A1# set pseudowire-status-tlv
user@A1# set revert-time 10 maximum 60
user@A1# set backup-neighbor 192.168.0.102 virtual-circuit-id 2
user@A1# set backup-neighbor 192.168.0.102 hot-standby
```

7. To have the unicast next hop get pushed to other access routers, configure per-packet load balancing.

```
[edit policy-options policy-statement pplb]
user@A1# set then load-balance per-packet
```

8. Apply the per-packet load balancing policy.

```
[edit routing-options forwarding-table]
user@A1# set export pplb
```

9. Configure the autonomous system (AS) ID and the router ID.

```
[edit routing-options]
user@A1# set router-id 192.168.0.100
user@A1# set autonomous-system 64510
```

Similarly, configure any other access devices.

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 Device PE1:

1. Configure the interfaces.

Enable MPLS on the core-facing interfaces.

```
[edit interfaces]
user@PE1# set ge-0/1/1 unit 0 family inet address 10.21.0.101/24
user@PE1# set ge-0/1/1 unit 0 family iso
user@PE1# set ge-0/1/1 unit 0 family mpls
```

```
user@PE1# set ge-0/1/2 unit 0 family inet address 10.31.0.101/24
user@PE1# set ge-0/1/2 unit 0 family iso
user@PE1# set ge-0/1/2 unit 0 family mpls
```

```
user@PE1# set ge-0/1/3 unit 0 family inet address 10.10.0.101/24
user@PE1# set ge-0/1/3 unit 0 family iso
user@PE1# set ge-0/1/3 unit 0 family mpls
```

```
user@PE1# set lo0 unit 0 family inet address 192.168.0.101/32 primary
user@PE1# set lo0 unit 0 family iso address 49.0002.0192.0168.0003.00
user@PE1# set lo0 unit 1 family inet address 192.168.1.101/32
```


2. On Device PE1 and Device PE2, which are aggregation routers, configure a pair of logical tunnel interfaces to represent LT(x) and LT(y).

The solution uses logical tunnel (lt-) paired interfaces for stitching the Layer 2 and Layer 3 domains.

A Layer 2 pseudowire terminates on one of the logical tunnel interfaces, LT(x), defined with the circuit cross-connect (CCC) address family. A Layer 3 VPN terminates the second logical tunnel interface, LT(y), defined with the IPv4 (inet) address family. LT(x) and LT(y) are paired.

```
[edit interfaces]
```

```
user@PE1# set lt-1/2/0 unit 600 encapsulation vlan-ccc
user@PE1# set lt-1/2/0 unit 600 vlan-id 600
user@PE1# set lt-1/2/0 unit 600 peer-unit 601
```

```
user@PE1# set lt-1/2/0 unit 601 encapsulation vlan
user@PE1# set lt-1/2/0 unit 601 vlan-id 600
user@PE1# set lt-1/2/0 unit 601 peer-unit 600
user@PE1# set lt-1/2/0 unit 601 family inet filter input icmp_inet
user@PE1# set lt-1/2/0 unit 601 family inet filter output icmp_inet
```

3. (Optional) Associate a unique VRRP address with both Device PE1 and Device PE2.

In this case, both Device PE1 and Device PE2 assume the mastership state for the defined VIP IPv4 address, so no VRRP hello message are exchanged between the routers.

```
[edit interfaces lt-1/2/0 unit 601 family inet address 10.41.0.101/24]
user@PE1# set vrrp-group 0 virtual-address 10.41.0.1
user@PE1# set vrrp-group 0 accept-data
```

4. Configure IS-IS or another IGP.

```
[edit protocols isis]
user@PE1# set interface ge-0/1/1.0
user@PE1# set interface ge-0/1/2.0
user@PE1# set interface ge-0/1/3.0
user@PE1# set interface lo0.0
```

5. Configure the MPLS on the core-facing interfaces.

```
[edit protocols mpls]
user@PE1# set interface ge-0/1/1.0
user@PE1# set interface ge-0/1/2.0
user@PE1# set interface ge-0/1/3.0
```

6. Configure label-switched paths to the other PE devices.

BGP is a policy-driven protocol, so also configure and apply any needed routing policies. For example, you might want to export static routes into BGP.

```
[edit protocols mpls]
user@PE1# set label-switched-path to_PE3 to 192.168.0.103
user@PE1# set label-switched-path to_PE2 to 192.168.0.102
```

7. Configure LDP on the core-facing interfaces and on the loopback interface.

```
[edit protocols ldp]
user@PE1# set interface ge-0/1/1.0
```

```

user@PE1# set interface ge-0/1/2.0
user@PE1# set interface ge-0/1/3.0
user@PE1# set interface lo0.0

```

8. Configure RSVP on the core-facing interfaces and on the loopback interface.

```

[edit protocols rsvp]
user@PE1# set interface ge-0/1/1.0
user@PE1# set interface ge-0/1/2.0
user@PE1# set interface ge-0/1/3.0
user@PE1# set interface lo0.0

```

9. Configure internal BGP (IBGP).

```

[edit protocols bgp]
user@PE1# set local-address 192.168.0.101
user@PE1# set group ibgp family inet-vpn any
user@PE1# set group ibgp peer-as 64511
user@PE1# set group ibgp neighbor 192.168.0.102
user@PE1# set group ibgp neighbor 192.168.0.103

```

10. Configure the Layer 2 circuit on the logical tunnel interface.

Configure the **hot-standby-vc-on** statement if you want a hot standby pseudowire to be established upon arrival of PW_FWD_STDBY status TLV.

```

[edit protocols l2circuit neighbor 192.168.0.100 interface lt-1/2/0.600]
user@PE1# set virtual-circuit-id 1
user@PE1# set pseudowire-status-tlv hot-standby-vc-on

```

11. Define a pair of conditions to be applied to the egress policy defined within the Layer 3 VPN instance.

In both condition **primary** and condition **standby**, the matching route corresponds to the interface lt-1/2/0.600 (y), as this is the format in which egress routes appear in routing table mpls.0 to represent any given pseudowire.

The difference between these conditions is in the **standby** attribute. Upon arrival of the PW_FWD_STDBY status TLV to Device PE1 or Device PE2, Junos OS matches condition **standby**, and in consequence, only term **standby** within the **l3vpn** policy will be executed. On the other hand, if the PW_FWD_STDBY status TLV is not present, the policy only matches condition **primary**, which then executes term **primary** in the **l3vpn** policy. Also, for logical tunnel-based CCC services, you must specify the logical tunnel interface, LT(y), that is associated with the logical tunnel CCC interface, LT(x). (See [“Understanding Pseudowire Redundancy Mobile Backhaul Scenarios” on page 367.](#))

Finally, for CCC-based conditions, Junos OS only allows mpls.0 as the matching routing table. For the **address** attribute, Junos OS only allows strings with a logical interface unit format (for example, lt-0/0/0.0).

```

[edit policy-options condition primary if-route-exists address-family ccc]
user@PE1# set lt-1/2/0.600
user@PE1# set table mpls.0
user@PE1# set peer-unit 601

```

```

[edit policy-options condition standby if-route-exists address-family ccc]
user@PE1# set lt-1/2/0.600

```

```

user@PE1# set table mpls.0
user@PE1# set standby
user@PE1# set peer-unit 601

```

12. Configure the Layer 3 VPN export policy.

If the Layer 2 virtual circuit (VC) is primary, the corresponding provider edge (PE) routing device advertises the attachment circuit's (AC's) subnet with the higher local preference. All aggregation PE devices initially advertise the AC's subnet with the same local preference.

This routing policy allows a higher local preference value to be advertised if the Layer 2 VC is active.

```

[edit policy-options policy-statement l3vpn_export]
user@PE1# set term primary from condition primary
user@PE1# set term primary then local-preference add 300
user@PE1# set term primary then community set l3vpn
user@PE1# set term primary then accept

```

```

user@PE1# set term standby from condition standby
user@PE1# set term standby then local-preference add 30
user@PE1# set term standby then community set l3vpn
user@PE1# set term standby then accept

```

```

user@PE1# set term default then community set l3vpn
user@PE1# set term default then accept

```

13. Configure the Layer 3 VPN community members.

```

[edit policy-options community l3vpn]
user@PE1# set members target:64511:600

```

14. Configure the Layer 3 VPN import policy, based on the Layer 3 VPN community.

```

[edit policy-options policy-statement l3vpn_import]
user@PE1# set term 1 from community l3vpn
user@PE1# set term 1 then accept
user@PE1# set term default then reject

```

15. Configure OSPF export policy, based on the Layer 3 VPN community.

```

[edit policy-options policy-statement ospf_export term 0]
user@PE1# set from community l3vpn
user@PE1# set then accept

```

16. (Optional) Configure a firewall filter to check the path taken by traffic.

```

[edit firewall family inet filter icmp_inet]
user@PE1# set interface-specific
user@PE1# set term 0 from source-address 10.41.0.101/32 except
user@PE1# set term 0 from source-address 10.0.0.0/8
user@PE1# set term 0 from protocol icmp
user@PE1# set term 0 then count icmp_inet
user@PE1# set term 0 then log
user@PE1# set term 0 then accept
user@PE1# set term 1 then accept

```

17. Configure the routing instance.

This routing instance is in the Layer 2 domain where Device PE1 and Device PE2 are interconnected to the metro ring over multiaccess media (Ethernet). You must include the **vrf-table-label** statement on Device PE1 and Device PE2 to enable advertisement of the direct subnet prefix corresponding to the logical tunnel (lt-) interface toward the Layer 3 domain.

Device PE1 and Device PE2 use OSPF for Layer 3 VPN communication with Device CE1.

```
[edit routing-instances l3vpn]
user@PE1# set instance-type vrf
user@PE1# set interface lt-1/2/0.601
user@PE1# set interface lo0.1
user@PE1# set route-distinguisher 192.168.1.101:64511
user@PE1# set vrf-import l3vpn_import
user@PE1# set vrf-export l3vpn_export
user@PE1# set vrf-table-label
user@PE1# set protocols ospf export ospf_export
user@PE1# set protocols ospf area 0.0.0.0 interface lt-1/2/0.601
user@PE1# set protocols ospf area 0.0.0.0 interface lo0.1
```

18. Configure the autonomous system (AS) ID and router ID.

```
[edit routing-options]
user@PE1# set router-id 192.168.0.101
user@PE1# set autonomous-system 64511
```

Similarly, configure Device PE2.

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

```
Device A1 user@A1# show interfaces
ge-1/3/0 {
  unit 0 {
    family inet {
      address 10.20.0.100/24;
    }
    family iso;
    family mpls;
  }
}
ge-1/3/1 {
  unit 0 {
    family inet {
      address 10.10.0.100/24;
    }
    family iso;
    family mpls;
  }
}
ge-1/3/2 {
  vlan-tagging;
  encapsulation vlan-ccc;
```

```

    unit 600 {
        encapsulation vlan-ccc;
        vlan-id 600;
        family ccc;
    }
}
lo0 {
    unit 0 {
        family inet {
            address 192.168.0.100/32 {
                primary;
            }
        }
        family iso {
            address 49.0002.0192.0168.0100.00;
        }
    }
}

```

user@A1# show protocols

```

rsvp {
    interface ge-1/3/0.0;
    interface ge-1/3/1.0;
    interface lo0.0;
}
mpls {
    interface ge-1/3/0.0;
    interface ge-1/3/1.0;
}
isis {
    interface ge-1/3/0.0;
    interface ge-1/3/1.0;
    interface lo0.0;
}
ldp {
    interface ge-1/3/0.0;
    interface ge-1/3/1.0;
    interface lo0.0;
}
l2circuit {
    neighbor 192.168.0.101 {
        interface ge-1/3/2.600 {
            virtual-circuit-id 1;
            pseudowire-status-tlv;
            backup-neighbor 192.168.0.102 {
                virtual-circuit-id 2;
                hot-standby;
            }
        }
    }
}

```

user@A1# show policy-options

```

policy-statement pplb {
    then {
        load-balance per-packet;
    }
}

```

```

    }
  }

  user@A1# show routing-options
  autonomous-system 64510;
  router-id 192.168.0.100;
  forwarding-table {
    export pplb;
  }
}

Device PE1 user@PE1# show interfaces
ge-0/1/1 {
  unit 0 {
    family inet {
      address 10.21.0.101/24;
    }
    family iso;
    family mpls;
  }
}
ge-0/1/2 {
  unit 0 {
    family inet {
      address 10.31.0.101/24;
    }
    family iso;
    family mpls;
  }
}
ge-0/1/3 {
  unit 0 {
    family inet {
      address 10.10.0.101/24;
    }
    family iso;
    family mpls;
  }
}
lt-1/2/0 {
  unit 600 {
    encapsulation vlan-ccc;
    vlan-id 600;
    peer-unit 601;
  }
  unit 601 {
    encapsulation vlan;
    vlan-id 600;
    peer-unit 600;
    family inet {
      filter {
        input icmp_inet;
        output icmp_inet;
      }
    }
    address 10.41.0.101/24 {
      vrrp-group 0 {
        virtual-address 10.41.0.1;
        accept-data;
      }
    }
  }
}

```

```

    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 192.168.0.101/32 {
        primary;
      }
    }
    family iso {
      address 49.0002.0192.0168.0003.00;
    }
  }
  unit 1 {
    family inet {
      address 192.168.1.101/32;
    }
  }
}
}

```

```

user@PE1# show firewall
family inet {
  filter icmp_inet {
    interface-specific;
    term 0 {
      from {
        source-address {
          10.41.0.101/32 except;
          10.0.0.0/8;
        }
        protocol icmp;
      }
      then {
        count icmp_inet;
        log;
        accept;
      }
    }
    term 1 {
      then accept;
    }
  }
}

```

```

user@PE1# show protocols
rsvp {
  interface ge-0/1/1.0;
  interface ge-0/1/2.0;
  interface ge-0/1/3.0;
  interface lo0.0;
}
mpls {
  label-switched-path to_PE3 {

```

```
        to 192.168.0.103;
    }
    label-switched-path to_PE2 {
        to 192.168.0.102;
    }
    interface ge-0/1/1.0;
    interface ge-0/1/2.0;
    interface ge-0/1/3.0;
}
bgp {
    local-address 192.168.0.101;
    group ibgp {
        family inet-vpn {
            any;
        }
        peer-as 64511;
        neighbor 192.168.0.102;
        neighbor 192.168.0.103;
    }
}
isis {
    interface ge-0/1/1.0;
    interface ge-0/1/2.0;
    interface ge-0/1/3.0;
    interface lo0.0;
}
ldp {
    interface ge-0/1/1.0;
    interface ge-0/1/2.0;
    interface ge-0/1/3.0;
    interface lo0.0;
}
l2circuit {
    neighbor 192.168.0.100 {
        interface lt-1/2/0.600 {
            virtual-circuit-id 1;
            pseudowire-status-tlv hot-standby-vc-on;
        }
    }
}

user@PE1# show policy-options
policy-statement l3vpn_export {
    term primary {
        from condition primary;
        then {
            local-preference add 300;
            community set l3vpn;
            accept;
        }
    }
    term standby {
        from condition standby;
        then {
            local-preference add 30;
            community set l3vpn;
        }
    }
}
```



```

        accept;
    }
}
term default {
    then {
        community set l3vpn;
        accept;
    }
}
}
policy-statement l3vpn_import {
    term 1 {
        from community l3vpn;
        then accept;
    }
    term default {
        then reject;
    }
}
policy-statement ospf_export {
    term 0 {
        from community l3vpn;
        then accept;
    }
}
community l3vpn members target:64511:600;
condition primary {
    if-route-exists {
        address-family {
            ccc {
                lt-1/2/0.600;
                table mpls.0;
                peer-unit 601;
            }
        }
    }
}
condition standby {
    if-route-exists {
        address-family {
            ccc {
                lt-1/2/0.600;
                table mpls.0;
                standby;
                peer-unit 601;
            }
        }
    }
}
}

user@PE1# show routing-options
router-id 192.168.0.101;
autonomous-system 64511;

user@PE1# show routing-instances
l3vpn {
    instance-type vrf;

```

```

interface lt-1/2/0.601;
interface lo0.1;
route-distinguisher 192.168.1.101:64511;
vrf-import l3vpn_import;
vrf-export l3vpn_export;
vrf-table-label;
protocols {
  ospf {
    export ospf_export;
    area 0.0.0.0 {
      interface lt-1/2/0.601;
      interface lo0.1;
    }
  }
}
}

```

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

Verification

Confirm that the configuration is working properly.

- [Checking Layer 2 Circuits on page 390](#)
- [Checking the Policy Conditions on page 392](#)

Checking Layer 2 Circuits

Purpose Upon Layer 2 virtual circuit (VC) establishment, the output of the **show l2circuit connections** command shows the active and the hot-standby VC. In addition, control-plane details are shown for the hot-standby VC.

Action From operational mode, enter the **show l2circuit connections extensive** command.

```
user@A1> show l2circuit connections extensive
```

Layer-2 Circuit Connections:

Legend for connection status (St)

EI -- encapsulation invalid	NP -- interface h/w not present
MM -- mtu mismatch	Dn -- down
EM -- encapsulation mismatch	VC-Dn -- Virtual circuit Down
CM -- control-word mismatch	Up -- operational
VM -- vlan id mismatch	CF -- Call admission control failure
OL -- no outgoing label	IB -- TDM incompatible bitrate
NC -- intf encaps not CCC/TCC	TM -- TDM misconfiguration
BK -- Backup Connection	ST -- Standby Connection
CB -- rcvd cell-bundle size bad	SP -- Static Pseudowire
LD -- local site signaled down	RS -- remote site standby
RD -- remote site signaled down	HS -- Hot-standby Connection
XX -- unknown	

Legend for interface status

Up -- operational
Dn -- down

Neighbor: 192.168.0.101

Interface	Type	St	Time last up	# Up trans
-----------	------	----	--------------	------------

```

ge-1/3/2.600(vc 1)      rmt  Up    Jan 24 11:00:26 2013      1
  Remote PE: 192.168.0.101, Negotiated control-word: Yes (Null)
  Incoming label: 299776, Outgoing label: 299776
  Negotiated PW status TLV: Yes
  Local PW status code: 0x00000000, Neighbor PW status code: 0x00000000
  Local interface: ge-1/3/2.600, Status: Up, Encapsulation: VLAN
Connection History:
  Jan 24 11:00:26 2013  status update timer
  Jan 24 11:00:26 2013  PE route changed
  Jan 24 11:00:26 2013  Out lbl Update                      299776
  Jan 24 11:00:26 2013  In lbl Update                      299776
  Jan 24 11:00:26 2013  loc intf up                        ge-1/3/2.600
Neighbor: 192.168.0.102
Interface              Type  St    Time last up      # Up trans
ge-1/3/2.600(vc 2)    rmt  HS    -----          ----
  Remote PE: 192.168.0.102, Negotiated control-word: Yes (Null)
  Incoming label: 299792, Outgoing label: 299776
  Negotiated PW status TLV: Yes
  Local PW status code: 0x00000020, Neighbor PW status code: 0x00000000
  Local interface: ge-1/3/2.600, Status: Up, Encapsulation: VLAN

```

user@PE1> show l2circuit connections extensive

Layer-2 Circuit Connections:

Legend for connection status (St)

EI -- encapsulation invalid	NP -- interface h/w not present
MM -- mtu mismatch	Dn -- down
EM -- encapsulation mismatch	VC-Dn -- Virtual circuit Down
CM -- control-word mismatch	Up -- operational
VM -- vlan id mismatch	CF -- Call admission control failure
OL -- no outgoing label	IB -- TDM incompatible bitrate
NC -- intf encaps not CCC/TCC	TM -- TDM misconfiguration
BK -- Backup Connection	ST -- Standby Connection
CB -- rcvd cell-bundle size bad	SP -- Static Pseudowire
LD -- local site signaled down	RS -- remote site standby
RD -- remote site signaled down	HS -- Hot-standby Connection
XX -- unknown	

Legend for interface status

Up -- operational
Dn -- down

Neighbor: 192.168.0.100

```

Interface              Type  St    Time last up      # Up trans
lt-1/2/0.600(vc 1)    rmt  Up    Jan 24 11:06:36 2013      1
  Remote PE: 192.168.0.100, Negotiated control-word: Yes (Null)
  Incoming label: 299776, Outgoing label: 299776
  Negotiated PW status TLV: Yes
  Local PW status code: 0x00000000, Neighbor PW status code: 0x00000000
  Local interface: lt-1/2/0.600, Status: Up, Encapsulation: VLAN
Connection History:
  Jan 24 11:06:36 2013  status update timer
  Jan 24 11:06:36 2013  PE route changed
  Jan 24 11:06:36 2013  Out lbl Update                      299776
  Jan 24 11:06:36 2013  In lbl Update                      299776
  Jan 24 11:06:36 2013  loc intf up                        lt-1/2/0.600

```

user@PE2> show l2circuit connections extensive

Layer-2 Circuit Connections:

Legend for connection status (St)

```

EI -- encapsulation invalid      NP -- interface h/w not present
MM -- mtu mismatch              Dn -- down
EM -- encapsulation mismatch    VC-Dn -- Virtual circuit Down
CM -- control-word mismatch     Up -- operational
VM -- vlan id mismatch         CF -- Call admission control failure
OL -- no outgoing label        IB -- TDM incompatible bitrate
NC -- intf encaps not CCC/TCC  TM -- TDM misconfiguration
BK -- Backup Connection        ST -- Standby Connection
CB -- rcvd cell-bundle size bad SP -- Static Pseudowire
LD -- local site signaled down RS -- remote site standby
RD -- remote site signaled down HS -- Hot-standby Connection
XX -- unknown

```

Legend for interface status

Up -- operational

Dn -- down

Neighbor: 192.168.0.100

```

Interface      Type St   Time last up      # Up trans
1t-1/2/0.600(vc 2)  rmt  Up   Jan 24 10:55:31 2013      1
Remote PE: 192.168.0.100, Negotiated control-word: Yes (Null)
Incoming label: 299776, Outgoing label: 299792
Negotiated PW status TLV: Yes
Local PW status code: 0x00000000, Neighbor PW status code: 0x00000020
Local interface: 1t-1/2/0.600, Status: Up, Encapsulation: VLAN
Connection History:
Jan 24 10:55:31 2013 status update timer
Jan 24 10:55:31 2013 PE route changed
Jan 24 10:55:31 2013 Out lbl Update                299792
Jan 24 10:55:31 2013 In lbl Update                  299776
Jan 24 10:55:31 2013 loc intf up                    1t-1/2/0.600

```

Meaning From the perspective of Device PE1 and Device PE2, a single Layer 2 circuit is established toward access routers, so there is no standby device information in the CLI output of the **show l2circuit connections** command. Note that no timing and flapping information is provided for the VC acting as the hot-standby. Junos OS only allows these counters to be tracked for the active VC.

Checking the Policy Conditions

Purpose On the PE devices, verify the state of the different conditions defined as part of the Layer3 VPN's egress policy, where 10.41.0.0/24 corresponds to the logical tunnel (y) subnet.

Action From operational mode, enter the **show policy conditions detail** command.

```
user@PE1> show policy conditions detail
```

Configured conditions:

Condition primary (static), event: Existence of a route in a specific routing table

Dependent routes:

10.41.0.0/24, generation 8

192.168.0.104/32, generation 8

Condition standby (static), event: Existence of a route in a specific routing table

Dependent routes:

None

```
Condition tables:
Table mpls.0, generation 0, dependencies 0, If-route-exists conditions: primary
(static) standby (static)
Table l3vpn.inet.0, generation 12, dependencies 2

user@PE2> show policy conditions detail
Configured conditions:
Condition primary (static), event: Existence of a route in a specific routing
table
Dependent routes:
  10.41.0.0/24, generation 18

Condition standby (static), event: Existence of a route in a specific routing
table
Dependent routes:
  10.41.0.0/24, generation 18

Condition tables:
Table mpls.0, generation 0, dependencies 0, If-route-exists conditions: primary
(static) standby (static)
Table l3vpn.inet.0, generation 367, dependencies 2
```

Related Documentation

- [Understanding Pseudowire Redundancy Mobile Backhaul Scenarios on page 367](#)

Configuring Load Balancing for Layer 2 Circuits

- [Reducing APS Switchover Time in Layer 2 Circuits on page 395](#)

Reducing APS Switchover Time in Layer 2 Circuits

On M320 routers with Channelized OC3/STM1 Circuit Emulation PIC with SFP, you can configure the **fast-aps-switch** statement at the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level to reduce the Automatic Protection Switching (APS) switchover time in Layer 2 circuits. Configuring this statement reduces the APS switchover time only when the Layer 2 circuit encapsulation type for the interface receiving traffic from a Layer 2 circuit neighbor is Structure Agnostic time-division multiplexing (TDM) over Packet (SAToP).

The **fast-aps-switch** statement must be configured on both working and protect circuits. Additionally, to achieve reduction in APS switchover time:

- Per-packet load balancing must be configured.
- Bidirectional switching mode must be configured.
- If the **fast-aps-switch** statement is configured in revertive APS mode, configure an appropriate value for revert time. We recommend that you configure a revert time of 600 seconds for 672 through 1344 Layer 2 circuits.
- To prevent the logical interfaces in the data path from being shut down, configure appropriate hold-time values on all the interfaces in the data path that support TDM.



NOTE:

- The **fast-aps-switch** statement cannot be configured when the APS annex-b option is configured.
 - The interfaces that have the **fast-aps-switch** statement configured cannot be used in virtual private LAN service (VPLS) environments.
-

The following tasks illustrate how to configure Junos OS to reduce APS switchover time.



NOTE: Per-packet load balancing can be configured for a limited set of routes or for all routes. To simplify the steps involved in configuring per-packet load balancing, steps for configuring per-packet load balancing for all routes is covered in this procedure.

- [Configuring Per-Packet Load Balancing on page 396](#)
- [Configuring Fast APS Switchover on page 396](#)

Configuring Per-Packet Load Balancing

To configure per-packet load balancing for all routes:

1. Configure the **per-packet** option for the **load-balance** statement at the **[edit policy-options policy-statement *policy-name* then]** hierarchy level.

```
[edit policy-options policy-statement policy-name then]
user@host# set load-balance per-packet
```

For example:

```
[edit policy-options policy-statement load-balancing-policy then]
user@host# set load-balance per-packet
```

2. Configure the policy name in the **export** statement at the **[edit routing-options forwarding-table]** hierarchy level.

```
[edit routing-options forwarding-table]
user@host# set export policy-name
```

For example:

```
[edit routing-options forwarding-table]
user@host# set export load-balancing-policy
```

Configuring Fast APS Switchover

To configure fast APS switchover:

1. On both the working and protect circuits, configure the **fast-aps-switch** statement at the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level.

```
[edit interfaces interface-name sonet-options aps]
user@host# set fast-aps-switch
```

For example:

```
[edit interfaces cstm1-0/0/0 sonet-options aps]
user@host# set fast-aps-switch
```

```
[edit interfaces cstm1-0/1/0 sonet-options aps]
user@host# set fast-aps-switch
```

2. Configure bidirectional switching mode on both the working and protect circuits. To do this, configure the **switching-mode bidirectional** statement at the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level on both the working and protect circuits.


```
[edit interfaces interface-name sonet-options aps]
user@host# set switching-mode bidirectional
```

For example:

```
[edit interfaces cstm1-0/0/0 sonet-options aps]
user@host# set switching-mode bidirectional
```

```
[edit interfaces cstm1-0/1/0 sonet-options aps]
user@host# set switching-mode bidirectional
```

3. If APS is configured in revertive mode, configure an appropriate value for revert time on both the working and protect circuits. To do this, configure the **revert-time** statement at the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level on both the working and protect circuits.

```
[edit interfaces interface-name sonet-options aps]
user@host# set revert-time seconds
```

For example:

```
[edit interfaces cstm1-0/0/0 sonet-options aps]
user@host# set revert-time 600
```

```
[edit interfaces cstm1-0/1/0 sonet-options aps]
user@host# set revert-time 600
```

4. To prevent the logical interfaces in the data path from being shut down, configure appropriate hold-time values on *all* interfaces in the data path that support TDM.

```
[edit interfaces interface-name hold-time]
user@host# set up seconds down seconds
```

For example:

```
[edit interfaces cstm1-0/0/0 hold-time]
user@host# set up 1 down 400
```


CHAPTER 27

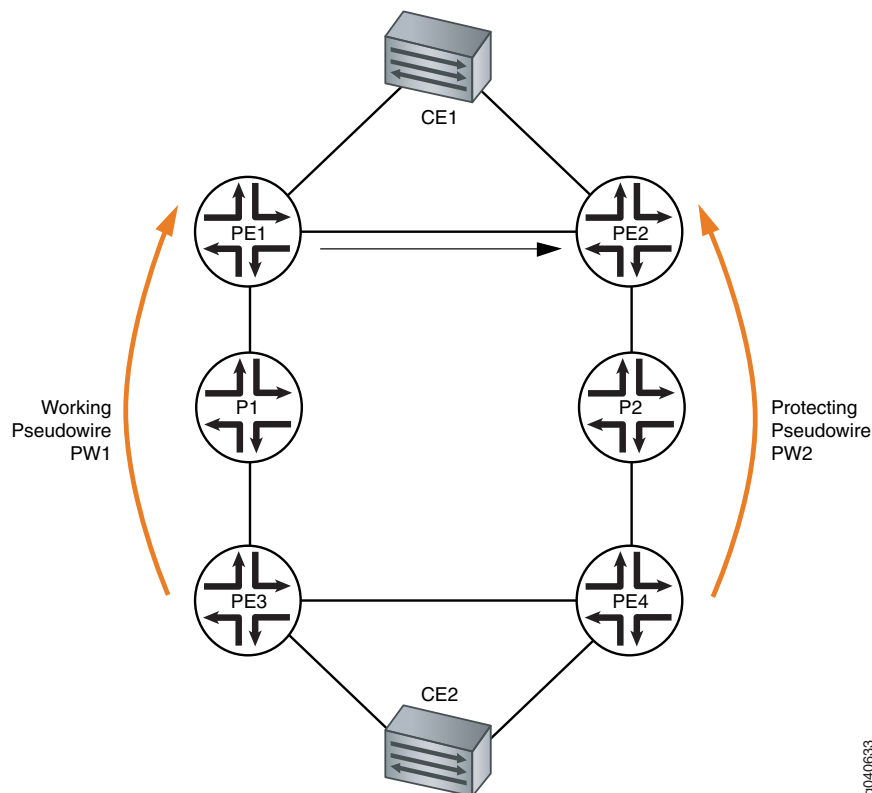
Configuring Protection Features for Layer 2 Circuits

- [Egress Protection LSPs for Layer 2 Circuits on page 399](#)
- [Configuring Egress Protection Service Mirroring for BGP Signaled Layer 2 Services on page 401](#)
- [Example: Configuring an Egress Protection LSP for a Layer 2 Circuit on page 404](#)
- [Example: Configuring Layer 2 Circuit Protect Interfaces on page 415](#)
- [Example: Configuring Layer 2 Circuit Switching Protection on page 420](#)

Egress Protection LSPs for Layer 2 Circuits

An egress protection LSP provides link protection for link between PE routers and CE devices as illustrated in [Figure 32 on page 400](#).

Figure 32: Egress Protection LSP



Device CE1 is multihomed to router PE1 and router PE2. Device CE2 is multihomed to router PE3 and router PE4. There are two paths connecting devices CE1 and CE2. The working path is CE2-PE3-P1-PE1-CE1, using pseudowire PW1. The protecting path is CE2-PE4-P2-PE2-CE1, using pseudowire PW2. Normally, traffic flows through the working path. When the end-to-end OAM between devices CE1 and CE2 detects a failure on the working path, traffic will be switched from the working path to the protecting path.

In the topology shown in [Figure 32 on page 400](#), if there was a link or node failure in the core network (for example, a link failure from router P1 to PE1, from router PE3 to P1, or a node failure of router P1), MPLS fast reroute can be triggered on the transport LSPs between router PE3 and router PE1 to repair the connection within tens of milliseconds. Egress protection LSPs address the problem of when a link failure occurs at the edge of the network (for example, a link failure on router PE1 to device CE1).

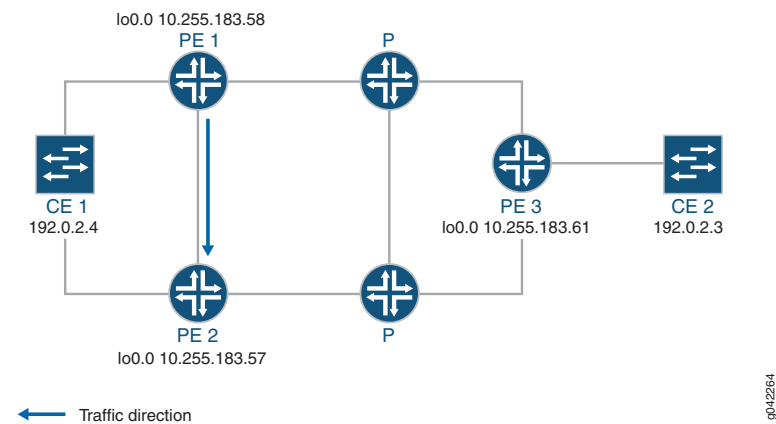
An egress protection LSP has been configured from router PE1 to router PE2. In the event of a link failure between router PE1 and device CE1, traffic can be switched to the egress protection LSP. Traffic from device CE2 can now be routed through path PE3-P1-PE1-PE2 to reach device CE1.

Configuring Egress Protection Service Mirroring for BGP Signaled Layer 2 Services

If there is a link or node failure in the core network, a protection mechanism such as MPLS fast reroute can be triggered on the transport LSPs between the PE routers to repair the connection within tens of milliseconds. An egress protection LSP addresses the problem of a node-link failure at the edge of the network (for example, a failure of a PE router).

Figure 1 shows a simplified topology of the use case that explains this feature.

Figure 33: Egress Protection LSP Configured from Router PE1 to Router PE2



CE1 is multihomed to PE1 and PE2. There are two paths connecting CE1 and CE2. The working path is CE2-PE3-P-PE1-CE1, via pseudowire PW21. The protecting path is CE2-PE3-P-PE2-CE1, via pseudowire PW22. Traffic is flowing through the working path under normal circumstances. When the end-to-end OAM between CE1 and CE2 detects failure on the working path, traffic will be switched from the working path to the protecting path. The end-to-end failure detection and recovery relies on control plane hence should be relatively slow. To achieve faster protection, local repair mechanisms similar to those used by MPLS fast reroute should be used. In Figure 1 above, if link or node failed in the core network (like link failure on P-PE1, P-PE3, or node failure on P), the MPLS fast reroute will happen on the transport LSPs between PE1 and PE3. The failure could be locally repaired within tens of milliseconds. However, if link or node failure happens at the edge (like link failure on PE3-CE2 or node failure on PE3), there is no local repair currently so we have to rely on the CE1-CE2 end-to-end protection to repair the failure.

- Device CE2—Traffic origin
- Router PE3—Ingress PE router
- Router PE1— (Primary) Egress PE router
- Router PE2—Protector PE router
- Device CE1—Traffic destination

When the link between CE1– PE1 goes down, PE1 will briefly redirect that traffic towards CE1, to PE2. PE2 forwards it to CE1 until ingress router PE3 recalculates to forward the traffic to PE2.

Initially the traffic direction was; CE2 – PE3 – P – PE1 – CE1.

When the link between CE1– PE1 goes down, the traffic will be; CE2 – PE3 – P – PE1 – PE2 – CE1. PE3 then recalculates the path; CE2 – PE3 – P – PE2 – CE1.

1. Configure RSVP on PE1, PE2, and PE3.

```
[edit protocols]
user@PE1# set interface all
user@PE2# set interface all
user@PE3# set interface all
```

2. Configure MPLS.

```
[edit protocols mpls]
user@PE1# set interface all
user@PE2# set interface all
user@PE3# set interface all
```

3. Set PE1 as **primary** and PE2 as **protector** nodes.

```
[edit protocols mpls]
user@PE1# set egress-protection context-identifier address primary
user@PE2# set egress-protection context-identifier address protector
```

4. Enable **egress-protection** on PE1 and PE2.

```
[edit protocols bgp]
user@PE1# set group ibgp family l2vpn egress-protection
user@PE2# set group ibgp family l2vpn egress-protection
```

5. Configure LDP and ISIS on PE1, PE2, and PE3.

```
[edit protocols ldp]
user@PE1# set interface all
user@PE2# set interface all
user@PE3# set interface all

[edit protocols isis]
user@PE1# set interface all point-to-point
user@PE2# set interface all point-to-point
user@PE3# set interface all point-to-point
```

6. Configure a load balancing policy at PE1, PE2, and PE3.

```
[edit]
user@PE1# set policy-options policy-statement lb then load-balance per-packet
user@PE2# set policy-options policy-statement lb then load-balance per-packet
user@PE3# set policy-options policy-statement lb then load-balance per-packet
```

7. Configure the routing options at PE1, PE2, and PE3, to export routes based on the load balancing policy.

```
[edit]
user@PE1# set routing-options traceoptions file ro.log
user@PE1# set routing-options traceoptions flag normal
user@PE1# set routing-options traceoptions flag route
```

```

user@PE1# set routing-options autonomous-system 100
user@PE1# set routing-options forwarding-table export lb

```

```

[edit]
user@PE2# set routing-options traceoptions file ro.log
user@PE2# set routing-options traceoptions flag normal
user@PE2# set routing-options traceoptions flag route
user@PE2# set routing-options autonomous-system 100
user@PE2# set routing-options forwarding-table export lb

```

```

[edit]
user@PE3# set routing-options traceoptions file ro.log
user@PE3# set routing-options traceoptions flag normal
user@PE3# set routing-options traceoptions flag route
user@PE3# set routing-options autonomous-system 100
user@PE3# set routing-options forwarding-table export lb

```

8. Configure BGP at PE1 to advertise nrli from the routing instance with context-ID as next-hop.

```

[edit]
user@PE1# set routing-instances foo egress-protection context-identifier
context-identifier

```

9. Configure l2vpn at PE1, PE2, and PE3

At PE1:

```

[edit routing-instances]
foo {
  instance-type l2vpn;
  egress-protection {
    context-identifier {
      192.0.2.1;
    }
  }
  interface ge-2/0/2.0;
  route-distinguisher 10.255.183.58:1;
  vrf-target target:9000:1;
  protocols {
    l2vpn {
      encapsulation-type ethernet-vlan;
      site foo {
        site-identifier 1;
        multi-homing;
        site-preference primary;
        interface ge-2/0/2.0 {
          remote-site-id 2;
        }
      }
    }
  }
}

```

At PE2:

```

[edit routing-instances]
foo {
  instance-type l2vpn;

```

```

egress-protection {
  protector;
}
interface ge-2/0/2.0;
route-distinguisher 10.255.183.57:1;
vrf-target target:9000:1;
protocols {
  l2vpn {
    encapsulation-type ethernet-vlan;
    site foo {
      site-identifier 1;
      multi-homing;
      site-preference backup;
      interface ge-2/0/2.0 {
        remote-site-id 2;
      }
    }
  }
}
}

```

At PE3:

```

[edit routing-instances]
foo {
  instance-type l2vpn;
  interface ge-2/1/2.0;
  route-distinguisher 10.255.183.61:1;
  vrf-target target:9000:1;
  protocols {
    l2vpn {
      encapsulation-type ethernet-vlan;
      site foo {
        site-identifier 2;
        interface ge-2/1/2.0;
      }
    }
  }
}

```

Related Documentation

- [\[edit routing-instances\] Hierarchy Level](#)
- [Example: Configuring MPLS Egress Protection Service Mirroring for BGP Signaled Layer 2 Services on page 471](#)
- [site-preference on page 1196](#)

Example: Configuring an Egress Protection LSP for a Layer 2 Circuit

This example shows how to configure an egress protection LSP.

- [Requirements on page 405](#)
- [Egress Protection LSP Overview on page 405](#)
- [Egress Protection LSP Configuration on page 406](#)

Requirements

Egress protection LSPs are supported on Juniper Networks MX Series routers only. This requirement applies to the PE routers facilitating the egress protection LSP.

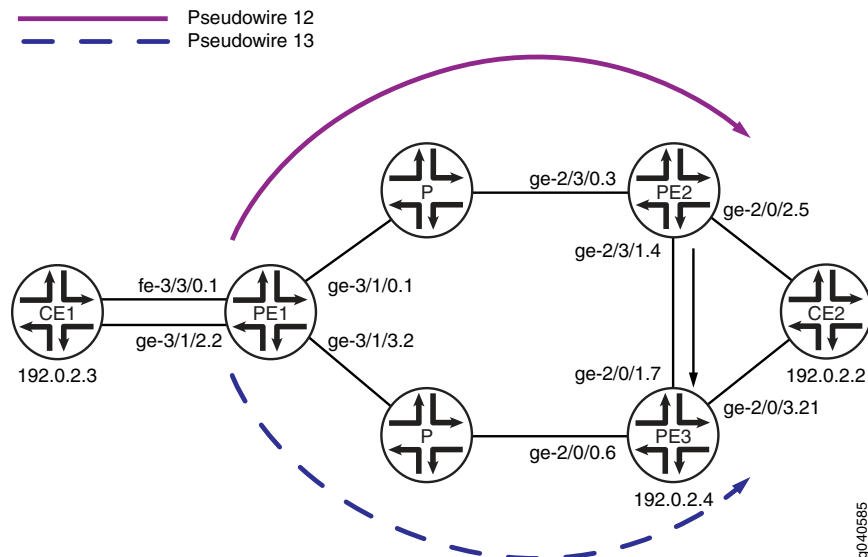
Egress Protection LSP Overview

If there is a link or node failure in the core network, a protection mechanism such as MPLS fast reroute can be triggered on the transport LSPs between the PE routers to repair the connection within tens of milliseconds. An egress protection LSP addresses the problem of when a link failure occurs at the edge of the network (for example, a link failure between a PE router and a CE device). Egress protection LSPs do not address the problem of a node failure at the edge of the network (for example, a failure of a PE router). An egress protection LSP is an RSVP-signaled ultimate hop popping LSP.

This example includes the following configuration concepts and statements that are unique to the configuration of an egress protection LSP:

- **context-identifier**—Specifies an IPV4 address used to define the pair of PE routers participating in the egress protection LSP. The context identifier is used to assign an identifier to the protector PE router. The identifier is propagated to the other PE routers participating in the network, making it possible for the protected egress PE router to signal the egress protection LSP to the protector PE router.
- **egress-protection**—Configures the protector information for the protected Layer 2 circuit and configures the protector Layer 2 circuit at the **[edit protocols l2circuit]** hierarchy level. Configures an LSP as an egress protection LSP at the **[edit protocols mpls label-switched-path lsp-name]** hierarchy level. It also configures the context identifier at the **[edit protocols mpls]** hierarchy level.
- **protected-l2circuit**—Specifies which Layer 2 circuit is to be protected by the egress protect LSP. This statement includes the following sub-statements: **ingress-pe**, **egress-pe**, and **virtual-circuit-id**. These sub-statements specify the address of the PE router at the ingress of the Layer 2 circuit, the address of the PE router at the egress of the Layer 2 circuit, and the Layer 2 circuit's identifier respectively.
- **protector-interface**—Specify the interface used by the egress protection LSP. In the event of a local link failure to a CE device, the egress protect LSP uses the interface specified to communicate with the protector PE router.
- **protector-pe**—Specify the IPv4 address of the protector PE router. The protector PE router must have a connection to the same CE device as the protected PE router for the egress protect LSP to function. This statement includes the following sub-statements: **context-identifier** and **lsp**. The **lsp** statement specifies the LSP to be used as the actual egress protection LSP.

Figure 34: Egress Protection LSP Configured from Router PE2 to Router PE3



Pseudowires are configured along two paths, one from router PE1 to router PE2 (pseudowire 12) and one from router PE1 to router PE3 (pseudowire 13). In the event of a failure on the link between router PE2 and device CE2, traffic is switched to the egress protection LSP configured between router PE2 and router PE3 (the protector PE router):

- Device CE1—Traffic origin
- Router PE1—Ingress PE router
- Router PE2—Egress PE router
- Router PE3—Protector PE router
- Device CE2—Traffic destination

This example shows how to configure routers PE1, PE2, and PE3.

Egress Protection LSP Configuration

- [Step-by-Step Procedure on page 408](#)
- [Results on page 412](#)

CLI Quick Configuration

To quickly configure an egress protection LSP, copy the following commands into a text file, modify the interface configurations to match your equipment, remove any line breaks, and then paste the commands into the CLI. This group of set commands is for router PE1.

```
set protocols rsvp interface ge-3/1/0.1
set protocols rsvp interface ge-3/1/3.2
set protocols mpls interface ge-3/1/0.1
set protocols mpls interface ge-3/1/3.2
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface ge-3/1/0.1
set protocols ospf area 0.0.0.0 interface ge-3/1/3.2
set protocols ospf area 0.0.0.0 interface lo0.0 passive
```

```

set protocols ldp interface ge-3/1/0.1
set protocols ldp interface ge-3/1/3.2
set protocols ldp interface lo0.0
set protocols l2circuit neighbor 192.0.2.3 interface fe-3/3/0.1 virtual-circuit-id 32
set protocols l2circuit neighbor 192.0.2.3 interface fe-3/3/0.1 egress-protection
  protector-interface ge-3/1/2.2
set protocols l2circuit neighbor 192.0.2.4 interface ge-3/1/2.2 virtual-circuit-id 33
set policy-options policy-statement load-balance-example then load-balance per-packet
set routing-options router-id 192.0.2.2
set routing-options forwarding-table export load-balance-example

```

To quickly configure an egress protection LSP, copy the following commands into a text file, modify the interface configurations to match your equipment, remove any line breaks, and then paste the commands into the CLI. This group of set commands is for router PE2.

```

[edit]
set protocols rsvp tunnel-services
set protocols rsvp interface ge-2/3/0.3
set protocols rsvp interface ge-2/3/1.4 link-protection
set protocols ldp interface ge-2/3/0.3
set protocols ldp interface ge-2/3/1.4
set protocols ldp interface lo0.0
set protocols ldp upstream-label-assignment
set protocols mpls label-switched-path protected-lsp to 192.0.2.5
set protocols mpls label-switched-path protected-lsp egress-protection
set protocols mpls interface ge-2/3/0.3
set protocols mpls interface ge-2/3/1.4
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface ge-2/3/0.3
set protocols ospf area 0.0.0.0 interface ge-2/3/1.4
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols l2circuit neighbor 192.0.2.2 interface ge-2/0/2.5 virtual-circuit-id 23
set protocols l2circuit neighbor 192.0.2.2 interface ge-2/0/2.5 egress-protection
  protector-pe 192.0.2.4
set protocols l2circuit neighbor 192.0.2.2 interface ge-2/0/2.5 egress-protection
  protector-pe context-identifier 192.0.2.5
set policy-options policy-statement load-balance-example then load-balance per-packet
set routing-options router-id 192.0.2.3
set routing-options forwarding-table export load-balance-example

```

To quickly configure an egress protection LSP, copy the following commands into a text file, modify the interface configurations to match your equipment, remove any line breaks, and then paste the commands into the CLI. This group of set commands is for router PE3.

```

set protocols rsvp tunnel-services
set protocols rsvp interface ge-2/0/0.6
set protocols rsvp interface ge-2/0/1.7
set protocols mpls interface ge-2/0/0.6
set protocols mpls interface ge-2/0/1.7
set protocols mpls egress-protection context-identifier 192.0.2.5 protector
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface ge-2/0/0.6
set protocols ospf area 0.0.0.0 interface ge-2/0/1.7
set protocols ospf area 0.0.0.0 interface lo0.0 passive

```

```
set protocols ldp interface ge-2/0/0.6
set protocols ldp interface ge-2/0/1.7
set protocols ldp interface lo0.0
set protocols ldp upstream-label-assignment
set protocols l2circuit neighbor 192.0.2.2 interface ge-2/0/3.21 virtual-circuit-id 42
set protocols l2circuit neighbor 192.0.2.2 interface ge-2/0/3.21 egress-protection
protected-l2circuit PW1
set protocols l2circuit neighbor 192.0.2.2 interface ge-2/0/3.21 egress-protection
protected-l2circuit ingress-pe 192.0.2.2
set protocols l2circuit neighbor 192.0.2.2 interface ge-2/0/3.21 egress-protection
protected-l2circuit egress-pe 192.0.2.3
set protocols l2circuit neighbor 192.0.2.2 interface ge-2/0/3.21 egress-protection
protected-l2circuit virtual-circuit-id 31
```

Step-by-Step Procedure

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 an egress protection LSP, complete the following steps for router PE1:

1. Configure RSVP. Include the interface linked to router PE2 and the interface linked to router PE3.

```
[edit]
user@PE1# edit protocols rsvp
[edit protocols rsvp]
user@PE1# set interface ge-3/1/0.1
[edit protocols rsvp]
user@PE1# set interface ge-3/1/3.2
```

2. Configure LDP. Include the interface linked to router PE2, the interface linked to router PE3, and the loopback interface.

```
[edit]
user@PE1# edit protocols ldp
[edit protocols ldp]
user@PE1# set interface ge-3/1/0.1
[edit protocols ldp]
user@PE1# set interface ge-3/1/3.2
[edit protocols ldp]
user@PE1# set interface lo0.0
```

3. Configure MPLS. Include the interface linked to router PE2 and the interface linked to router PE3.

```
[edit]
user@PE1# edit protocols mpls
[edit protocols mpls]
user@PE1# set interface ge-3/1/0.1
[edit protocols mpls]
user@PE1# set interface ge-3/1/3.2
```

4. Configure OSPF. Include the interface linked to router PE2, the interface linked to router PE3, and the loopback interface in the configuration for the OSPF area.

```
[edit]
user@PE1# edit protocols ospf
[edit protocols ospf]
user@PE1# set interface traffic-engineering
[edit protocols ospf]
user@PE1# set area 0.0.0.0 interface ge-3/1/0.1
[edit protocols ospf]
user@PE1# set area 0.0.0.0 interface ge-3/1/3.2
[edit protocols ospf]
user@PE1# set area 0.0.0.0 interface lo0.0 passive
```

5. Configure Layer 2 circuits to use the egress protection LSP to protect against a link failure to device CE1.

```
[edit]
user@PE1# edit protocols l2circuit
[edit protocols l2circuit]
user@PE1# set neighbor 192.0.2.3 interface fe-3/3/0.1 virtual-circuit-id 32
[edit protocols l2circuit]
user@PE1# edit neighbor 192.0.2.3
[edit protocols l2circuit neighbor 192.0.2.3]
user@PE1# set interface fe-3/3/0.1 egress-protection protector-interface ge-3/1/2.2
[edit protocols l2circuit]
user@PE1# set neighbor 192.0.2.4 interface ge-3/1/2.2 virtual-circuit-id 33
```

6. Configure a load balancing policy.

```
[edit]
user@PE1# set policy-options policy-statement load-balance-example then
load-balance per-packet
```

7. Configure the routing options to export routes based on the load balancing policy.

```
[edit]
user@PE1# set routing-options router-id 192.0.2.2
[edit]
user@PE1# set routing-options forwarding-table export load-balance-example
```

8. If you are done configuring the device, commit the 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*.

To configure an egress protection LSP, complete the following steps for router PE2:

1. Configure RSVP. Include the interface linked to the ingress PE router and the interface linked to the CE device.

```
[edit]
user@PE2# edit protocols rsvp
[edit protocols rsvp]
user@PE2# set tunnel-services
[edit protocols rsvp]
user@PE2# set interface ge-2/3/0.3
[edit protocols rsvp]
user@PE2# set interface ge-2/3/1.4 link-protection
```

2. Configure LDP. Include the interface linked to the ingress PE router and the interface linked to the CE device.

```
[edit]
user@PE2# edit protocols ldp
[edit protocols ldp]
user@PE2# set interface ge-2/3/0.3
[edit protocols ldp]
user@PE2# set interface ge-2/3/1.4
[edit protocols ldp]
user@PE2# set interface lo0.0
[edit protocols ldp]
user@PE2# set upstream-label-assignment
```

3. Configure MPLS and the LSP which acts as the egress protection LSP.

```
[edit]
user@PE2# edit protocols mpls
[edit protocols mpls]
user@PE2# set interface ge-2/3/0.3
[edit protocols mpls]
user@PE2# set interface ge-2/3/1.4
[edit protocols mpls]
user@PE2# set label-switched-path protected-lsp to 192.0.2.5
[edit protocols mpls]
user@PE2# set label-switched-path protected-lsp egress-protection
```

4. Configure OSPF.

```
[edit]
user@PE2# edit protocols ospf
[edit protocols ospf]
user@PE2# set interface traffic-engineering
[edit protocols ospf]
user@PE2# set interface area 0.0.0.0 interface ge-2/3/0.3
[edit protocols ospf]
user@PE2# set interface area 0.0.0.0 interface ge-2/3/1.4
[edit protocols ospf]
user@PE2# set interface area 0.0.0.0 interface lo0.0 passive
```

5. Configure the Layer 2 circuit to use the egress protection LSP.

```
[edit]
user@PE2# edit protocols l2circuit
[edit protocols l2circuit]
user@PE2# set neighbor 192.0.2.2 interface ge-2/0/2.5 virtual-circuit-id 23
[edit protocols l2circuit]
user@PE2# edit neighbor 192.0.2.2
[edit protocols l2circuit neighbor 192.0.2.2]
user@PE2# set interface ge-2/0/2.5 egress-protectionprotector-pe 192.0.2.4
[edit protocols l2circuit neighbor 192.0.2.2]
user@PE2# set interface ge-2/0/2.5 egress-protection protector-pe
context-identifier 192.0.2.5
```

6. Configure a load balancing policy.

```
[edit]
user@PE1# set policy-options policy-statement load-balance-example then
load-balance per-packet
```

7. Configure the routing options to export routes based on the load balancing policy.

```
[edit]
user@PE2# set routing-options router-id 192.0.2.3
[edit]
user@PE2# set routing-options forwarding-table export load-balance-example
```

8. If you are done configuring the device, commit the configuration.

Step-by-Step Procedure

To configure an egress protection LSP, complete the following steps for router PE3:

1. Configure RSVP. Include the interface linked to the ingress PE router and the interface linked to the CE device.

```
[edit]
user@PE3# edit protocols rsvp
[edit protocols rsvp]
user@PE3# set tunnel-services
[edit protocols rsvp]
user@PE3# set interface ge-2/0/0.6
[edit protocols rsvp]
user@PE3# set interface ge-2/0/1.7
```

2. Configure LDP. Include the interface linked to the ingress PE router and the interface linked to the CE device.

```
[edit]
user@PE3# edit protocols ldp
[edit protocols ldp]
user@PE3# set interface ge-2/0/0.6
[edit protocols ldp]
user@PE3# set interface ge-2/0/1.7
[edit protocols ldp]
user@PE3# set interface lo0.0
[edit protocols ldp]
user@PE3# set upstream-label-assignment
```

3. Configure MPLS and the LSP which acts as the egress protection LSP.

```
[edit]
user@PE3# edit protocols mpls
[edit protocols mpls]
user@PE3# set interface ge-2/0/0.6
[edit protocols mpls]
user@PE3# set interface ge-2/0/1.7
[edit protocols mpls]
user@PE3# set egress-protection context-identifier 192.0.2.5 protector
```

4. Configure OSPF.

```
[edit]
user@PE3# edit protocols ospf
[edit protocols ospf]
user@PE3# set interface traffic-engineering
[edit protocols ospf]
user@PE3# set area 0.0.0.0 interface ge-2/0/0.6
[edit protocols ospf]
user@PE3# set area 0.0.0.0 interface ge-2/0/1.7
```

```
[edit protocols ospf]
user@PE3# set area 0.0.0.0 interface lo0.0 passive
```

5. Configure the Layer 2 circuit to use the egress protection LSP.

```
[edit]
user@PE3# edit protocols l2circuit
[edit protocols l2circuit]
user@PE3# set neighbor 192.0.2.2 interface ge-2/0/3.21 virtual-circuit-id 42
[edit protocols l2circuit]
user@PE3# edit neighbor 192.0.2.2
[edit protocols l2circuit neighbor 192.0.2.2]
user@PE3# set interface ge-2/0/3.21 egress-protection protected-l2circuit ingress-pe
192.0.2.2
[edit protocols l2circuit neighbor 192.0.2.2]
user@PE3# set interface ge-2/0/3.21 egress-protection protected-l2circuit egress-pe
192.0.2.3
[edit protocols l2circuit neighbor 192.0.2.2]
user@PE3# set interface ge-2/0/3.21 egress-protection
protected-l2circuit virtual-circuit-id 31
```

6. If you are done configuring the device, commit the configuration.

Results

From configuration mode, confirm your configuration on router PE1 by entering the **show protocols**, **show policy-options**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@PE1# show protocols
rsvp {
  interface ge-3/1/0.1;
  interface ge-3/1/3.2;
}
mpls {
  interface ge-3/1/0.1;
  interface ge-3/1/3.2;
}
ospf {
  traffic-engineering;
  area 0.0.0.0 {
    interface ge-3/1/0.1;
    interface ge-3/1/3.2;
    interface lo0.0 {
      passive;
    }
  }
}
ldp {
  interface ge-3/1/0.1;
  interface ge-3/1/3.2;
  interface lo0.0;
}
l2circuit {
```



```

neighbor 192.0.2.3 {
  interface fe-3/3/0.1 {
    virtual-circuit-id 32;
    egress-protection {
      protector-interface ge-3/1/2.2;
    }
  }
}
neighbor 192.0.2.4 {
  interface ge-3/1/2.2 {
    virtual-circuit-id 33;
  }
}
[edit]
user@PE1# show policy-options
policy-statement load-balance-example {
  then {
    load-balance per-packet;
  }
}
[edit]
user@PE1# show routing-options
router-id 192.0.2.2;
forwarding-table {
  export load-balance-example;
}

```

From configuration mode, confirm your configuration on router PE2 by entering the **show protocols**, **show policy-options**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
user@PE2# show protocols
rsdp {
  tunnel-services;
  interface ge-2/3/0.3;
  interface ge-2/3/1.4 {
    link-protection;
  }
}
mpls {
  label-switched-path protected-lsp {
    to 192.0.2.5;
    egress-protection;
  }
  interface ge-2/3/0.3;
  interface ge-2/3/1.4;
}
ospf {
  traffic-engineering;
  area 0.0.0.0 {
    interface ge-2/3/0.3;
    interface ge-2/3/1.4;
    interface lo0.0 {

```

```
        passive;
    }
}
}
ldp {
    interface ge-2/3/0.3;
    interface ge-2/3/1.4;
    interface lo0.0;
    upstream-label-assignment;
}
l2circuit {
    neighbor 192.0.2.2 {
        interface ge-2/0/2.5 {
            virtual-circuit-id 23;
            egress-protection {
                protector-pe 192.0.2.4 context-identifier 192.0.2.5;
            }
        }
    }
}
}

[edit]
user@PE2# show policy-options
policy-options {
    policy-statement load-balance-example {
        then {
            load-balance per-packet;
        }
    }
}

[edit]
user@PE2# show routing-options
routing-options {
    router-id 192.0.2.3;
    forwarding-table {
        export load-balance-example;
    }
}
}
```

From configuration mode, confirm your configuration on router PE3 by entering the **show protocols** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@PE3# show protocols
rsvp {
    tunnel-services;
    interface ge-2/0/0.6;
    interface ge-2/0/1.7;
}
mpls {
    interface ge-2/0/0.6;
    interface ge-2/0/1.7;
    egress-protection {
        context-identifier 192.0.2.5 {
            protector;
        }
    }
}
```

```

    }
  }
}
ospf {
  traffic-engineering;
  area 0.0.0.0 {
    interface ge-2/0/0.6;
    interface ge-2/0/1.7;
    interface lo0.0 {
      passive;
    }
  }
}
ldp {
  interface ge-2/0/0.6;
  interface ge-2/0/1.7;
  interface lo0.0;
  upstream-label-assignment;
}
l2circuit {
  neighbor 192.0.2.2 {
    interface ge-2/0/3.21 {
      virtual-circuit-id 42;
      egress-protection {
        protected-l2circuit PW1 ingress-pe 192.0.2.2 egress-pe 192.0.2.3 virtual-circuit-id
        31;
      }
    }
  }
}
}

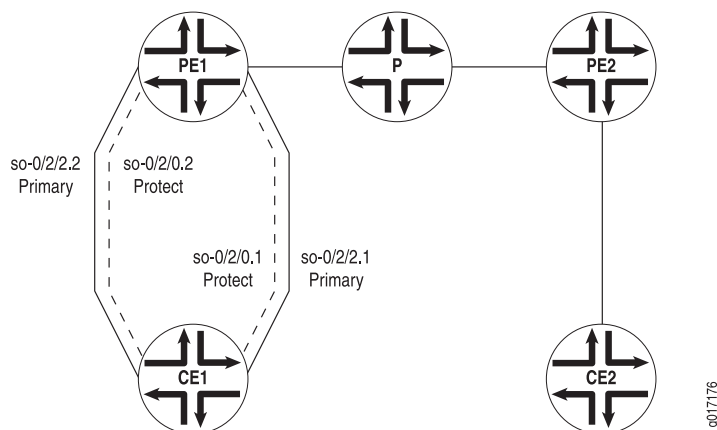
```

Example: Configuring Layer 2 Circuit Protect Interfaces

This example illustrates how you might configure a Layer 2 circuit with protect interfaces. Protect interfaces act as backups for their associated interfaces. The primary interface has priority over the protect interface and carries network traffic as long as it is functional. If the primary interface fails, the protect interface is activated. These interfaces can also share the same virtual path identifier (VPI) or virtual circuit identifier (VCI).

[Figure 35 on page 416](#) shows the network topology used in this example.

Figure 35: Layer 2 Circuits Using Protect Interfaces



The following sections describe how to configure a Layer 2 circuit to use a protect interface:

- [Configuring Router PE1 on page 416](#)
- [Configuring Router PE2 on page 418](#)
- [Configuring Router CE1 on page 419](#)
- [Configuring Router CE2 on page 420](#)

Configuring Router PE1

Configure an interface for traffic to Router CE1 from Router PE1 at the **[edit interfaces]** hierarchy level:

```
[edit interfaces]
so-0/2/2 {
  description "Router CE1 so-0/2/2";
  no-keepalives;
  encapsulation frame-relay-ccc;
  unit 1 {
    encapsulation frame-relay-ccc;
    point-to-point;
    dlci 600;
  }
  unit 2 {
    encapsulation frame-relay-ccc;
    point-to-point;
    dlci 602;
  }
}
```

Configure an interface for traffic to Router CE1 from Router PE1 at the **[edit interfaces]** hierarchy level. Logical interface **so-0/2/0.2** acts as the protect interface for **so-0/2/2.2**, and logical interface **so-0/2/0.1** acts as the protect interface for **so-0/2/2.1**:

```
[edit interfaces]
so-0/2/0 {
  description "to Router CE1 so-0/3/0";
```

```

no-keepalives;
encapsulation frame-relay-ccc;
unit 1 {
    encapsulation frame-relay-ccc;
    dlci 600;
}
unit 2 {
    encapsulation frame-relay-ccc;
    dlci 602;
}
}

```

Configure an interface for traffic to Router PE2 from Router PE1 at the **[edit interfaces]** hierarchy level:

```

[edit interfaces]
so-0/2/1 {
    description "to Router PE2 so-1/0/1";
    unit 0 {
        family inet {
            address 192.0.2.1/24 {
                destination 192.0.2.2;
            }
        }
        family iso;
        family mpls;
    }
}

```

Configure an interface for traffic to Router PE2 from Router PE1 at the **[edit interfaces]** hierarchy level:

```

[edit interfaces]
so-0/2/3 {
    description "Router PE2 so-1/0/3";
    unit 0 {
        family inet;
        family iso;
        family mpls;
    }
    lo0 {
        unit 0 {
            family inet {
                address 192.0.2.3/24;
                address 192.0.2.4/24;
            }
            family iso {
                address 47.0005.80ff.f800.0000.0108.0001.1921.6800.4213.00;
            }
        }
    }
}

```

Configure the Layer 2 circuit by including the **l2circuit** statement at the **[edit protocols]** hierarchy level. The logical interfaces for the Layer 2 circuits and their corresponding protect interfaces are included here:

```
[edit protocols]
l2circuit {
  neighbor 10.100.40.210 {
    interface so-0/2/2.2 {
      protect-interface so-0/2/0.2;
      virtual-circuit-id 2;
      no-control-word;
    }
    interface so-0/2/2.1 {
      protect-interface so-0/2/0.1;
      virtual-circuit-id 1;
      no-control-word;
    }
  }
}
```

Configuring Router PE2

Configure an interface for traffic to Router CE2 from Router PE2:

```
[edit interfaces]
so-1/0/0 {
  description "to Router CE2 so-0/2/0";
  no-keepalives;
  encapsulation frame-relay-ccc;
  unit 1 {
    encapsulation frame-relay-ccc;
    point-to-point;
    dlci 700;
  }
  unit 2 {
    encapsulation frame-relay-ccc;
    point-to-point;
    dlci 702;
  }
}
```

Configure an interface for traffic to Router PE1 from Router PE2:

```
[edit interfaces]
so-1/0/1 {
  description "to Router PE1 so-0/2/1";
  unit 0 {
    family inet {
      address 192.0.2.2/32 {
        destination 192.0.2.1;
      }
    }
    family iso;
    family mpls;
  }
}
```

Configure an interface for traffic to Router PE1 from Router PE2:

```
[edit interfaces]
so-1/0/3 {
```

```

description "to Router PE1 so-0/2/3";
unit 0 {
    family inet;
    family iso;
    family mpls;
}
}
lo0 {
    unit 0 {
        family inet {
            address 192.0.2.3/24;
            address 10.100.40.210/32;
        }
        family iso {
            address 47.0005.80ff.f800.0000.0108.0001.1921.6800.4216.00;
        }
    }
}
}

```

Configure the Layer 2 circuit at the **[edit protocols]** hierarchy level:

```

[edit protocols]
l2circuit {
    neighbor 192.0.2.4 {
        interface so-1/0/0.1 {
            virtual-circuit-id 1;
            no-control-word;
        }
        interface so-1/0/0.2 {
            virtual-circuit-id 2;
            no-control-word;
        }
    }
}
}

```

Configuring Router CE1

Configure an interface for traffic to Router PE1 from Router CE1:

```

[edit interfaces]
so-0/3/0 {
    description "to Router PE1 so-0/2/0";
    no-keepalives;
    encapsulation frame-relay;
    unit 1 {
        dlci 601;
        family inet {
            address 198.51.100.1/24;
        }
    }
}
}

```

Configure an interface for traffic to Router PE1 from Router CE1:

```

[edit interfaces]
so-0/3/1 {
    description "Router PE1 so-0/2/2";
}

```

```
no-keepalives;
encapsulation frame-relay;
unit 0 {
    dlc1 600;
    family inet {
        address 10.10.10.1/24;
        address 198.51.100.2/24;
    }
    family iso;
    family mpls;
}
unit 2 {
    dlc1 602;
    family inet {
        address 198.51.100.3/24;
    }
}
}
```

Configuring Router CE2

Configure an interface for traffic to Router PE2 from Router CE2:

```
[edit interfaces]
so-0/2/0 {
    description "to Router PE2 so-1/0/0";
    no-keepalives;
    encapsulation frame-relay;
    unit 1 {
        dlc1 700;
        family inet {
            address 10.10.10.2/24;
            address 198.51.100.4/24;
            address 198.51.100.5/24;
        }
    }
    unit 2 {
        dlc1 702;
        family inet {
            address 198.51.100.6/24;
        }
    }
}
```

Example: Configuring Layer 2 Circuit Switching Protection

Unlike Layer 2 circuit protect interfaces (see [“Example: Configuring Layer 2 Circuit Protect Interfaces” on page 415](#)), which provide traffic protection for paths configured between the PE routers and CE routers, Layer 2 circuit switching protection provides traffic protection for the paths configured between the PE routers. In the event the path used by a Layer 2 circuit fails, traffic can be switched to an alternate path (or protection path). Switching protection is supported for locally switched Layer 2 circuits and provides 1 to 1 protection for each Layer 2 circuit interface.

When you enable Layer 2 circuit switching protection, each Layer 2 circuit interface requires the following paths:

- Working path—Used by the Layer 2 circuit when working normally.
- Protection path—Used by the Layer 2 circuit when the working path fails.
- [Requirements on page 421](#)
- [Overview on page 421](#)
- [Configuration on page 422](#)

Requirements

This example uses the following hardware and software components:

- MX Series 3D Universal Edge Routers
- Junos OS Release 12.3

Overview

Each working path can be configured to have either a protection path routed directly to the neighboring PE router (as shown in [Figure 36 on page 421](#)) or indirectly using a pseudowire configured through an intermediate PE router (as shown in [Figure 37 on page 422](#) and [Figure 38 on page 422](#)). The protection path provides failure protection for the traffic flowing between the PE routers. Ethernet OAM monitors the status of these paths. When OAM detects a failure, it reroutes the traffic from the failed working path to the protection path. You can configure OAM to revert the traffic automatically to the working path when it is restored. You can also manually switch traffic between the working path, the protection path, and back.

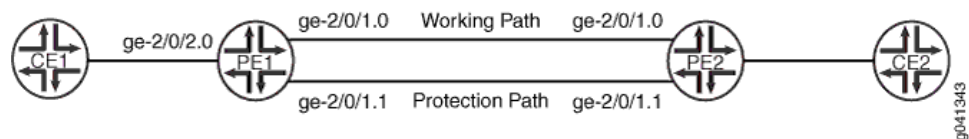


NOTE: Non-stop routing (NSR) and graceful routing engine switchover (GRES) do not support Layer 2 circuit switching protection.

Topology

[Figure 36 on page 421](#) illustrates Layer 2 circuit local switching. There are two OAM sessions running between Router PE1 and Router PE2. One OAM session is configured over the working path and the other is configured over the protection path.

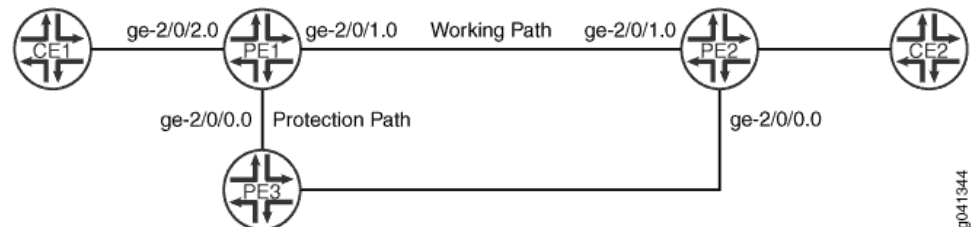
Figure 36: Connection Protection Enabled Between Router PE1 and Router PE2



In [Figure 37 on page 422](#) and [Figure 38 on page 422](#), there are two OAM sessions running between Router PE1 and Router PE2. For Figure 2, one OAM session is configured over

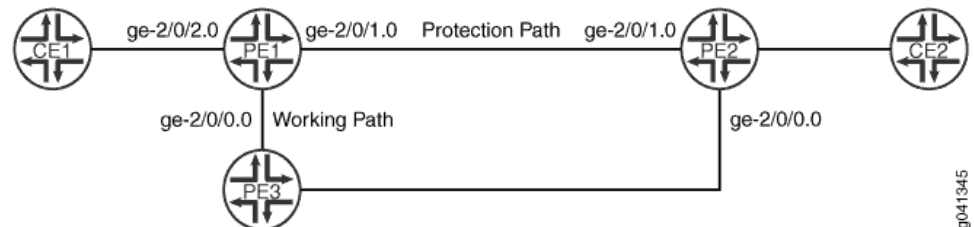
the working path between Router PE1 and Router PE2. The other OAM session is configured over the protection path between Router PE1 and Router PE3 to Router PE2.

Figure 37: Connection Protection Using a Pseudowire Configured through Router PE3 as the Protection Path



For [Figure 38 on page 422](#), one OAM session is configured over the working path, the pseudowire between Router PE1 and Router PE3, then to Router PE2. The other OAM session is configured on the protect path between Router PE1 and Router PE2.

Figure 38: Connection Protection Using a Pseudowire Configured through Router PE3 as the Working Path



Configuration

The following sections describe how to configure each of the variations of Layer 2 circuit connection protection:

- [Configuring Connection Protection Between Two PE Routers on page 422](#)
- [Configuring Connection Protection Using Another PE Router for the Protection Path on page 426](#)
- [Configuring Connection Protection Using an Another PE Router for the Working Path on page 429](#)

Configuring Connection Protection Between Two PE Routers

Step-by-Step Procedure

To configure Layer 2 Circuit switching protection as shown in [Figure 36 on page 421](#) on Router PE1:

1. Configure the Layer 2 circuit on Router PE1.

```
[edit protocols l2circuit]
user@PE1# set local-switching interface ge-2/0/2.0 connection-protection
user@PE1# set local-switching interface ge-2/0/2.0 end-interface interface
ge-2/0/1.0
user@PE1# set local-switching interface ge-2/0/2.0 end-interface backup-interface
ge-2/0/1.1
```

2. Configure the routing policy on Router PE1.


```
[edit policy-options]
user@PE1# set policy-statement protection-policy then load-balance per-packet
```
3. Enable the routing policy on Router PE1.


```
[edit routing-options]
user@PE1# set forwarding-table export protection-policy
```
4. Configure OAM on Router PE1. OAM is used to monitor the working path between Router PE1 and Router PE2. In the event of a failure on the working path, traffic is switched automatically to the protection path. A connectivity fault management (CFM) session is configured on the working path and on the protection path. Begin by configuring the OAM maintenance domain.


```
[edit protocols oam ethernet]
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md level 5
```
5. Configure OAM on Router PE1 for the working path.


```
[edit protocols oam ethernet]
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working continuity-check interval
100ms
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 1000 interface
ge-2/0/1.0
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 1000 interface
working
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 1000 direction down
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 1000 remote-mep
103
```
6. Configure OAM on Router PE1 for the protection path.


```
[edit protocols oam ethernet]
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection continuity-check
interval 100ms
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 1001 interface
ge-2/0/1.1
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 1001 interface
protect
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 1001 direction
down
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 1001 remote-mep
104
```
7. Configure the OAM maintenance domain on Router PE2.

```
[edit protocols oam ethernet]
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md level 5
```

8. Configure OAM on Router PE2 for the working path.

```
[edit protocols oam ethernet]
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working continuity-check interval
100ms
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 103 interface
ge-2/0/1.0
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 103 interface working
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 103 direction down
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 103 remote-mep
1000
```

9. Configure OAM on Router PE2 for the protection path.

```
[edit protocols oam ethernet]
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection continuity-check
interval 100ms
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 104 interface
ge-2/0/1.1
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 104 interface
protect
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 104 direction
down
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 104 remote-mep
1001
```

Results From configuration mode on Router PE1, confirm your configuration by entering the **show protocols l2circuit**, **show policy-options**, **show routing-options**, and **show protocols oam ethernet** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host> show protocols l2circuit
local-switching {
  interface ge-2/0/2.0 {
    connection-protection;
  end-interface {
    interface ge-2/0/1.0;
    backup-interface ge-2/0/1.1;
  }
}
}
user@host> show policy-options
```

```

policy-statement protection-policy {
  then {
    load-balance per-packet;
  }
}

user@host> show routing-options
forwarding-table {
  export protection-policy;
}

user@host> show protocols oam ethernet
connectivity-fault-management {
  maintenance-domain l2circuit-example-md {
    level 5;
    maintenance-association working {
      continuity-check {
        interval 100ms;
      }
      mep 1000 {
        interface ge-2/0/1.0 working;
        direction down;
        remote-mep 103;
      }
    }
  }
  maintenance-association protection {
    continuity-check {
      interval 100ms;
    }
    mep 1001 {
      interface ge-2/0/1.1 protect;
      direction down;
      remote-mep 104;
    }
  }
}
}

```

From configuration mode on Router PE2, confirm your configuration by entering the **show protocols oam ethernet** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

connectivity-fault-management {
  maintenance-domain l2circuit-example-md {
    level 5;
    maintenance-association working {
      continuity-check {
        interval 100ms;
      }
      mep 103 {
        interface ge-2/0/1.0 working;
        direction down;
        remote-mep 1000;
      }
    }
  }
  maintenance-association protection {
    continuity-check {

```

```

        interval 100ms;
    }
    mep 104 {
        interface ge-2/0/1.1 protect;
        direction down;
        remote-mep 1001;
    }
}
}
}

```

Configuring Connection Protection Using Another PE Router for the Protection Path

Step-by-Step Procedure To configure Layer 2 Circuit switching protection as shown in [Figure 37 on page 422](#) on Router PE1:

1. Configure the Layer 2 circuit on Router PE1.


```

[edit protocols l2circuit]
user@PE1# set local-switching interface ge-2/0/2.0 connection-protection
user@PE1# set local-switching interface ge-2/0/2.0 backup-neighbor 192.0.2.2
virtual-circuit-id 2
user@PE1# set local-switching interface ge-2/0/2.0 backup-neighbor 192.0.2.2
community example
user@PE1# set local-switching interface ge-2/0/2.0 end-interface interface
ge-2/0/1.0
      
```
2. Configure the routing policy on Router PE1.


```

[edit policy-options]
user@PE1# set policy-statement load-balance then load-balance per-packet
user@PE1# set policy-statement protection-policy term protect from community
example
user@PE1# set policy-statement protection-policy term protect then install-nexthop
lsp-regex lsp-protect-*
      
```
3. Configure the routing options on Router PE1.


```

[edit routing-options]
user@PE1# set forwarding-table export load-balance
      
```
4. Configure OAM on Router PE1 to setup the maintenance domain. OAM is used to monitor the working path between Router PE1 and Router PE2. In the event of a failure on the working path, traffic is switched automatically to the protection path.


```

[edit protocols oam ethernet]
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md level 5
      
```
5. Configure OAM on Router PE1 for the working path.


```

[edit protocols oam ethernet]
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 1000 interface
ge-2/0/1.0
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 1000 direction down
      
```

```
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 1000 remote-mep
103
```

6. Configure OAM on Router PE1 for the protection path.

```
[edit protocols oam ethernet]
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 1001 interface
ge-2/0/0.0
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 1001 direction
down
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 1001 remote-mep
104
```

7. Configure OAM on Router PE2 to setup the maintenance domain.

```
[edit protocols oam ethernet]
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md level 5
```

8. Configure OAM on Router PE2 for the working path.

```
[edit protocols oam ethernet]
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 103 interface
ge-2/0/1.0
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 103 direction down
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 103 remote-mep
1000
```

9. Configure OAM on Router PE2 for the protection path.

```
[edit protocols oam ethernet]
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 104 interface
ge-2/0/0.0
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 104 direction
down
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 104 remote-mep
1001
```

Results From configuration mode on Router PE1, confirm your configuration by entering the **show protocols l2circuit**, **show policy-options**, **show routing-options**, and **show protocols oam ethernet** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host> show protocols l2circuit
local-switching {
  interface ge-2/0/2.0 {
    connection-protection;
    backup-neighbor 192.0.2.2 {
```

```
        virtual-circuit-id 2;
        community example;
    }
    end-interface {
        interface ge-2/0/1.0;
    }
}

user@host> show policy-options
policy-statement load-balance {
    then {
        load-balance per-packet;
    }
}
policy-statement protection-policy {
    term protect {
        from community example;
        then {
            install-nexthop lsp-regex lsp-protect-*;
        }
    }
}

user@host> show routing-options
forwarding-table {
    export load-balance;
}

user@host> show protocols oam ethernet
connectivity-fault-management {
    maintenance-domain l2circuit-example-md {
        level 5;
        maintenance-association working {
            mep 1000 {
                interface ge-2/0/1.0;
                direction down;
                remote-mep 103;
            }
        }
        maintenance-association protection {
            mep 1001 {
                interface ge-2/0/0.0;
                direction down;
                remote-mep 104;
            }
        }
    }
}
```

From configuration mode on Router PE2, confirm your configuration by entering the **show protocols oam ethernet** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
connectivity-fault-management {
    maintenance-domain l2circuit-example-md {
        level 5;
```



```

maintenance-association working {
  mep 103 {
    interface ge-2/0/1.0;
    direction down;
    remote-mep 1000;
  }
}
maintenance-association protection {
  mep 104 {
    interface ge-2/0/0.0;
    direction down;
    remote-mep 1001;
  }
}
}
}

```

Configuring Connection Protection Using an Another PE Router for the Working Path

Step-by-Step Procedure

To configure Layer 2 Circuit switching protection as shown in [Figure 38 on page 422](#) on Router PE1:

1. Configure the Layer 2 circuit on Router PE1.


```

[edit protocols l2circuit]
user@PE1# set neighbor 192.0.2.2 interface ge-2/0/2.0 virtual-circuit-id 2
user@PE1# set neighbor 192.0.2.2 interface ge-2/0/2.0 community example
user@PE1# set neighbor 192.0.2.2 interface ge-2/0/2.0 connection-protection
user@PE1# set neighbor 192.0.2.2 interface ge-2/0/2.0 backup-neighbor 192.0.2.3
virtual-circuit-id 3
user@PE1# set neighbor 192.0.2.2 interface ge-2/0/2.0 backup-neighbor 192.0.2.3
standby
      
```
2. Configure the policies on Router PE1.


```

[edit policy-options]
user@PE1# set policy-statement load-balance then load-balance per-packet
user@PE1# set policy-statement protection-policy term protect from community
example
user@PE1# set policy-statement protection-policy term protect then install-nexthop
lsp-regex lsp-primary
      
```
3. Configure the routing options on Router PE1.


```

[edit routing-options]
user@PE1# set forwarding-table export load-balance
      
```
4. Configure OAM on Router PE1 to setup the maintenance domain. OAM is used to monitor the working path between Router PE1 and Router PE2. In the event of a failure on the working path, traffic is switched automatically to the protection path.


```

[edit protocols oam ethernet]
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md level 5
      
```
5. Configure OAM on Router PE1 for the working path.

```
[edit protocols oam ethernet]
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 1000 interface
ge-2/0/0.0
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 1000 direction down
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 1000 remote-mep
103
```

6. Configure OAM on Router PE1 for the protection path.

```
[edit protocols oam ethernet]
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 1001 interface
ge-2/0/1.0
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 1001 direction
down
user@PE1# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 1001 remote-mep
104
```

7. Configure OAM on Router PE2 to setup the maintenance domain.

```
[edit protocols oam ethernet]
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md level 5
```

8. Configure OAM on Router PE2 for the working path.

```
[edit protocols oam ethernet]
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 103 interface
ge-2/0/0.0
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 103 direction down
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association working mep 103 remote-mep
1000
```

9. Configure OAM on Router PE2 for the protection path.

```
[edit protocols oam ethernet]
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 104 interface
ge-2/0/1.0
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 104 direction
down
user@PE2# set connectivity-fault-management maintenance-domain
l2circuit-example-md maintenance-association protection mep 104 remote-mep
1001
```

Results From configuration mode on Router PE1, confirm your configuration by entering the **show protocols l2circuit**, **show policy-options**, **show routing-options**, and **show protocols oam ethernet** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

user@host> show protocols l2circuit
neighbor 192.0.2.2 {
  interface ge-2/0/2.0 {
    virtual-circuit-id 2;
    community example;
    connection-protection;
    backup-neighbor 192.0.2.3 {
      virtual-circuit-id 3;
      standby;
    }
  }
}

user@host> show policy-options
policy-statement load-balance {
  then {
    load-balance per-packet;
  }
}
policy-statement protection-policy {
  term protect {
    from community example;
    then {
      install-nexthop lsp-regex lsp-primary;
    }
  }
}

user@host> show routing-options
forwarding-table {
  export load-balance;
}

user@host> show protocols oam ethernet
connectivity-fault-management {
  maintenance-domain l2circuit-example-md {
    level 5;
    maintenance-association working {
      mep 1000 {
        interface ge-2/0/0.0;
        direction down;
        remote-mep 103;
      }
    }
    maintenance-association protection {
      mep 1001 {
        interface ge-2/0/1.0;
        direction down;
        remote-mep 104;
      }
    }
  }
}

```

From configuration mode on Router PE2, confirm your configuration by entering the **show protocols oam ethernet** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
connectivity-fault-management {  
  maintenance-domain l2circuit-example-md {  
    level 5;  
    maintenance-association working {  
      mep 103 {  
        interface ge-2/0/0.0;  
        direction down;  
        remote-mep 1000;  
      }  
    }  
    maintenance-association protection {  
      mep 104 {  
        interface ge-2/0/1.0;  
        direction down;  
        remote-mep 1001;  
      }  
    }  
  }  
}
```

**Related
Documentation**

- [Example: Configuring Layer 2 Circuit Protect Interfaces on page 415](#)

Monitoring Layer 2 Circuits with BFD

- [Configuring BFD for VCCV for Layer 2 Circuits on page 433](#)
- [Example: Configuring BFD for VCCV for Layer 2 Circuits on page 435](#)

Configuring BFD for VCCV for Layer 2 Circuits

Bidirectional Forwarding Detection (BFD) support for virtual circuit connection verification (VCCV) allows you to configure a control channel for a pseudowire, in addition to the corresponding operations and management functions to be used over that control channel. BFD provides a low resource mechanism for the continuous monitoring of the pseudowire data path and for detecting data plane failures. This feature provides support for asynchronous mode BFD for VCCV as described in RFC 5885, *Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)*. You can also use a ping to detect pseudowire failures. However, the processing resources required for a ping are greater than what is needed for BFD. In addition, BFD is capable of detecting data plane failure faster than VCCV ping. BFD for pseudowires is supported for Layer 2 circuits (LDP-based).

Before you begin:

- Configure the device interfaces.

To configure BFD for VCCV:

1. Specify the threshold for the adaptation of the BFD session detection time.

```
[edit protocols l2circuit neighbor IP-address interface interface-name oam
bfd-liveness-detection]
user@host# set detection-time threshold milliseconds
```

For example, to set a detection time threshold of 40 milliseconds for OAM BFD liveness detection:

```
[edit protocols l2circuit neighbor 192.0.2.1 interface ge-1/1/9.0 oam
bfd-liveness-detection]
user@host# set detection-time threshold 40
```

2. Configure the virtual circuit ID for the Layer 2 circuit protocol.

```
[edit protocols l2circuit neighbor IP-address interface interface-name]
user@host# set virtual-circuit-id virtual-circuit-id
```

For example, to set the virtual circuit ID as 1 for OAM BFD liveness detection:

```
[edit protocols l2circuit neighbor 192.0.2.1 interface ge-1/1/9.0 oam  
  bfd-liveness-detection]  
user@host# set virtual-circuit-id 1
```

3. Configure the minimum interval after which the local routing device transmits hello packets and then expects to receive a reply from a neighbor with which it has established a BFD session for the Layer 2 circuit.

```
[edit protocols l2circuit neighbor IP-address interface interface-name oam  
  bfd-liveness-detection]  
user@host# set minimum-interval milliseconds
```

For example, to set a minimum interval of 300 milliseconds for OAM BFD liveness detection:

```
[edit protocols l2circuit neighbor 192.0.2.1 interface ge-1/1/9.0 oam  
  bfd-liveness-detection]  
user@host# set minimum-interval 300
```

4. Configure the minimum interval after which the local routing device must receive a reply from a neighbor with which it has established a BFD session for the Layer 2 circuit protocol.

```
[edit protocols l2circuit neighbor IP-address interface interface-name oam  
  bfd-liveness-detection]  
user@host# set minimum-receive-interval milliseconds
```

For example, to set a minimum receive interval of 10 milliseconds for OAM BFD liveness detection:

```
[edit protocols l2circuit neighbor 192.0.2.1 interface ge-1/1/9.0 oam  
  bfd-liveness-detection]  
user@host# set minimum-receive-interval 10
```

5. Configure the number of hello packets not received by a neighbor that causes the originating interface to be declared down for the Layer 2 circuit protocol.

```
[edit protocols l2circuit neighbor IP-address interface interface-name oam  
  bfd-liveness-detection]  
user@host# set multiplier number
```

For example, to set the multiplier as 3 for OAM BFD liveness detection:

```
[edit protocols l2circuit neighbor 192.0.2.1 interface ge-1/1/9.0 oam  
  bfd-liveness-detection]  
user@host# set multiplier 3
```

6. Configure to disable adaptation.

```
[edit protocols l2circuit neighbor IP-address interface interface-name oam  
  bfd-liveness-detection]  
user@host# set no-adaptation
```

7. Configure the minimum interval at which the local routing device transmits hello packets to a neighbor with which it has established a BFD session.

```
[edit protocols l2circuit neighbor IP-address interface interface-name oam  
  bfd-liveness-detection transmit-interval]  
user@host# set minimum-interval milliseconds
```

For example, to set a minimum transmit interval of 5 milliseconds for OAM BFD liveness detection:

```
[edit protocols l2circuit neighbor 192.0.2.1 interface ge-1/1/9.0 oam
  bfd-liveness-detection transmit-interval]
user@host# set minimum-interval 5
```

8. Specify the threshold for the adaptation of the BFD session transmit interval.

```
[edit protocols l2circuit neighbor IP-address interface interface-name oam
  bfd-liveness-detection transmit-interval]
user@host# set threshold milliseconds
```

For example, to set a transmit interval threshold of 30 milliseconds for OAM BFD liveness detection:

```
[edit protocols l2circuit neighbor 192.0.2.1 interface ge-1/1/9.0 oam
  bfd-liveness-detection transmit-interval]
user@host# set threshold 30
```

Related Documentation

- [Example: Configuring BFD for VCCV for Layer 2 Circuits on page 435](#)

Example: Configuring BFD for VCCV for Layer 2 Circuits

This example shows how to configure BFD for VCCV for Layer 2 circuits which enables faster detection of failure in the data path.

- [Requirements on page 435](#)
- [Overview on page 435](#)
- [Configuration on page 436](#)
- [Verification on page 440](#)

Requirements

This example uses the following hardware and software components:

- Two MX Series 3D Universal Edge Routers
- Junos OS Release 12.1 or later running on all devices

Overview

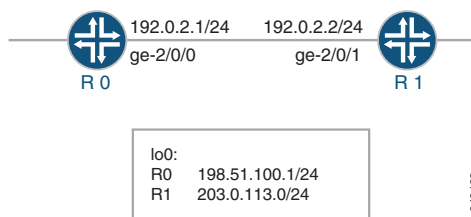
Starting with Junos OS Release 12.1, Bidirectional Forwarding Detection (BFD) support for virtual circuit connection verification (VCCV) allows you to configure a control channel for a pseudowire, in addition to the corresponding operations and management functions to be used over that control channel. BFD provides a low resource mechanism for the continuous monitoring of the pseudowire data path and for detecting data plane failures. This feature provides support for asynchronous mode BFD for VCCV as described in RFC 5885, *Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)*. You can also use a ping to detect pseudowire failures. However, the processing resources required for a ping are greater than what is needed

for BFD. In addition, BFD is capable of detecting data plane failure faster than VCCV ping. BFD for pseudowires is supported for Layer 2 circuits (LDP-based).

To configure BFD for VCCV for Layer 2 circuits, configure the **oam** configuration statement at the **[edit protocols l2circuit neighbor address interface interface-name]** hierarchy level. The **control-channel** configuration statement at the **[edit routing-instances routing-instance-name protocols l2vpn oam]** hierarchy level does not apply to Layer 2 circuit configurations.

Topology

In the topology, BFD for VCCV for Layer 2 circuits is configured on Device R0.



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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```

R0
set chassis redundancy graceful-switchover
set interfaces ge-1/1/9 vlan-tagging
set interfaces ge-1/1/9 encapsulation vlan-ccc
set interfaces ge-1/1/9 unit 0 encapsulation vlan-ccc
set interfaces ge-1/1/9 unit 0 vlan-id 512
set interfaces ge-2/0/0 unit 0 family inet address 192.0.2.1/24
set interfaces ge-2/0/0 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 198.51.100.0/24
set routing-options nonstop-routing
set routing-options static route 203.0.113.0/24 next-hop 192.0.2.2
set routing-options router-id 198.51.100.0
set protocols rsvp interface ge-2/0/0.0
set protocols mpls label-switched-path lsp1 to 203.0.113.0
set protocols mpls interface ge-2/0/0.0
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface ge-2/0/0.0
set protocols ldp interface all
set protocols l2circuit neighbor 203.0.113.0 interface ge-1/1/9.0 virtual-circuit-id 1
set protocols l2circuit neighbor 203.0.113.0 interface ge-1/1/9.0 oam bfd-liveness-detection
    minimum-interval 300
set protocols l2circuit neighbor 203.0.113.0 interface ge-1/1/9.0 oam bfd-liveness-detection
    minimum-receive-interval 10
set protocols l2circuit neighbor 203.0.113.0 interface ge-1/1/9.0 oam bfd-liveness-detection
    multiplier 3
  
```



```

set protocols l2circuit neighbor 203.0.113.0 interface ge-1/1/9.0 oam bfd-liveness-detection
  transmit-interval minimum-interval 5
set protocols l2circuit neighbor 203.0.113.0 interface ge-1/1/9.0 oam bfd-liveness-detection
  transmit-interval threshold 30
set protocols l2circuit neighbor 203.0.113.0 interface ge-1/1/9.0 oam bfd-liveness-detection
  detection-time threshold 40

```

```

R1  set interfaces ge-1/1/9 vlan-tagging
    set interfaces ge-1/1/9 encapsulation vlan-ccc
    set interfaces ge-1/1/9 unit 0 encapsulation vlan-ccc
    set interfaces ge-1/1/9 unit 0 vlan-id 512
    set interfaces ge-2/0/1 unit 0 family inet address 192.0.2.2/24
    set interfaces ge-2/0/1 unit 0 family mpls
    set interfaces lo0 unit 0 family inet address 203.0.113.0/24
    set routing-options static route 198.51.100.0/24 next-hop 192.0.2.1
    set routing-options router-id 203.0.113.0
    set protocols rsvp interface ge-2/0/1.0
    set protocols mpls label-switched-path lsp2 to 198.51.100.0
    set protocols mpls interface ge-2/0/1.0
    set protocols ospf traffic-engineering
    set protocols ospf area 0.0.0.0 interface ge-2/0/1.0
    set protocols ldp interface all
    set protocols l2circuit neighbor 198.51.100.0 interface ge-1/1/9.0 virtual-circuit-id 1
    set protocols l2circuit neighbor 198.51.100.0 interface ge-1/1/9.0 oam
      bfd-liveness-detection minimum-interval 300
    set protocols l2circuit neighbor 198.51.100.0 interface ge-1/1/9.0 oam
      bfd-liveness-detection minimum-receive-interval 10
    set protocols l2circuit neighbor 198.51.100.0 interface ge-1/1/9.0 oam
      bfd-liveness-detection multiplier 3
    set protocols l2circuit neighbor 198.51.100.0 interface ge-1/1/9.0 oam
      bfd-liveness-detection transmit-interval minimum-interval 5
    set protocols l2circuit neighbor 198.51.100.0 interface ge-1/1/9.0 oam
      bfd-liveness-detection transmit-interval threshold 30
    set protocols l2circuit neighbor 198.51.100.0 interface ge-1/1/9.0 oam
      bfd-liveness-detection detection-time threshold 40

```

Configuring Device R0

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 Device R0:



NOTE: Repeat this procedure for Device R1 after modifying the appropriate interface names, addresses, and any other parameters for the device.

1. Configure graceful switchover redundancy.

```

[edit chassis]
user@R0# set redundancy graceful-switchover

```
2. Configure the interfaces.

```
[edit interfaces]
user@R0# set ge-1/1/9 vlan-tagging
user@R0# set ge-1/1/9 encapsulation vlan-ccc
user@R0# set ge-1/1/9 unit 0 encapsulation vlan-ccc
user@R0# set ge-1/1/9 unit 0 vlan-id 512

user@R0# set ge-2/0/0 unit 0 family inet address 192.0.2.1/24
user@R0# set ge-2/0/0 unit 0 family mpls

user@R0# set lo0 unit 0 family inet address 198.51.100.0/24
```

3. Configure the nonstop routing option, the static route, and the router ID routing options.

```
[edit routing-options]
user@R0# set nonstop-routing
user@R0# set static route 203.0.113.0/24 next-hop 192.0.2.2
user@R0# set router-id 198.51.100.0
```

4. Configure the RSVP protocol.

```
[edit protocols rsvp]
user@R0# set interface ge-2/0/0.0
```

5. Configure the MPLS protocol.

```
[edit protocols mpls]
user@R0# set label-switched-path lsp1 to 203.0.113.0
user@R0# set interface ge-2/0/0.0
```

6. Configure the OSPF protocol.

```
[edit protocols ospf]
user@R0# set traffic-engineering
user@R0# set area 0.0.0.0 interface ge-2/0/0.0
```

7. Configure the LDP protocol.

```
[edit protocols ldp]
user@R0# set interface all
```

8. Configure the virtual circuit ID for the neighbor of Layer 2 circuit protocols.

```
[edit protocols l2circuit]
user@R0# set neighbor 203.0.113.0 interface ge-1/1/9.0 virtual-circuit-id 1
```

9. Configure the oam attributes of the Layer 2 circuit protocol.

```
[edit protocols l2circuit]
user@R0# set neighbor 203.0.113.0 interface ge-1/1/9.0 oam bfd-liveness-detection
  minimum-interval 300
user@R0# set neighbor 203.0.113.0 interface ge-1/1/9.0 oam bfd-liveness-detection
  minimum-receive-interval 10
user@R0# set neighbor 203.0.113.0 interface ge-1/1/9.0 oam bfd-liveness-detection
  multiplier 3
user@R0# set neighbor 203.0.113.0 interface ge-1/1/9.0 oam bfd-liveness-detection
  transmit-interval minimum-interval 5
user@R0# set neighbor 203.0.113.0 interface ge-1/1/9.0 oam bfd-liveness-detection
  transmit-interval threshold 30
```

```
user@R0# set neighbor 203.0.113.0 interface ge-1/1/9.0 oam bfd-liveness-detection
detection-time threshold 40
```

Results

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

```
user@R0# show chassis
redundancy {
  graceful-switchover;
}

user@R0# show interfaces
ge-1/1/9 {
  vlan-tagging;
  encapsulation vlan-ccc;
  unit 0 {
    encapsulation vlan-ccc;
    vlan-id 512;
  }
}
ge-2/0/0 {
  unit 0 {
    family inet {
      address 192.0.2.1/24;
    }
    family mpls;
  }
}
lo0 {
  unit 0 {
    family inet {
      address 198.51.100.0/24;
    }
  }
}

user@R0# show protocols
rsvp {
  interface ge-2/0/0.0;
}
mpls {
  label-switched-path lsp1 {
    to 203.0.113.0;
  }
  interface ge-2/0/0.0;
}
ospf {
  traffic-engineering;
  area 0.0.0.0 {
    interface ge-2/0/0.0;
  }
}
```

```
ldp {
  interface all;
}
l2circuit {
  neighbor 203.0.113.0 {
    interface ge-1/1/9.0 {
      virtual-circuit-id 1;
      oam {
        bfd-liveness-detection {
          minimum-interval 300;
          minimum-receive-interval 10;
          multiplier 3;
          transmit-interval {
            minimum-interval 5;
            threshold 30;
          }
          detection-time {
            threshold 40;
          }
        }
      }
    }
  }
}
}

user@R0# show routing-options
nonstop-routing;
static {
  route 203.0.113.0/24 next-hop 192.0.2.2;
}
router-id 198.51.100.0;
```

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

Verification

Verify that the configuration is working properly.

- [Verifying the Layer 2 Circuit Connections on page 440](#)
- [Verifying the BFD Session on page 441](#)
- [Verifying Detailed BFD Session Information on page 442](#)

Verifying the Layer 2 Circuit Connections

Purpose Verify the connections in a Layer 2 Circuit.

Action From operational mode, run the **show l2circuit connections** command for Device R0.

```
user@R0> show l2circuit connections
```

Layer-2 Circuit Connections:

Legend for connection status (St)

EI -- encapsulation invalid	NP -- interface h/w not present
MM -- mtu mismatch	Dn -- down
EM -- encapsulation mismatch	VC-Dn -- Virtual circuit Down
CM -- control-word mismatch	Up -- operational
VM -- vlan id mismatch	CF -- Call admission control failure
OL -- no outgoing label	IB -- TDM incompatible bitrate
NC -- intf encaps not CCC/TCC	TM -- TDM misconfiguration
BK -- Backup Connection	ST -- Standby Connection
CB -- rcvd cell-bundle size bad	SP -- Static Pseudowire
LD -- local site signaled down	RS -- remote site standby
RD -- remote site signaled down	HS -- Hot-standby Connection
XX -- unknown	

Legend for interface status

Up -- operational

Dn -- down

Neighbor: 203.0.113.0

Interface	Type	St	Time last up	# Up trans
ge-1/1/9.0(vc 1)	rmt	Up	Jun 2 03:19:44 2014	1

Remote PE: 203.0.113.0, Negotiated control-word: Yes (Null)
Incoming label: 299792, Outgoing label: 299792
Negotiated PW status TLV: No
Local interface: ge-1/1/9.0, Status: Up, Encapsulation: VLAN
Flow Label Transmit: No, Flow Label Receive: No
Flow Label Transmit: No, Flow Label Receive: No

Meaning The output shows the Layer 2 virtual circuit information from Device R0 to its neighbor.

Verifying the BFD Session

Purpose Verify the BFD session.

Action From operational mode, run the **show bfd session** command for Device R0.

```
user@R0> show bfd session
```

Address	State	Interface	Detect Time	Transmit Interval	Multiplier
192.168.0.1	Up	ge-2/0/0.0	0.030	0.010	3

1 sessions, 1 clients

Cumulative transmit rate 100.0 pps, cumulative receive rate 100.0 pps

Meaning The output shows the address, and the interface on which the BFD session is active. The state *Up* indicates that the BFD session is up. The BFD session has a time interval of 30 milliseconds to detect BFD control packets, the transmitting system has a time interval

of 10 milliseconds to send BFD control packets, and the transmitting system determines the detection time by multiplying 3 with the time interval. Total number of active BFD sessions and total number of clients that are hosting active BFD sessions. Cumulative transmit rate indicates the total number of BFD control packets transmitted, per second, on all active sessions and cumulative receive rate indicates the total number of BFD control packets received, per second, on all active sessions.

Verifying Detailed BFD Session Information

Purpose Verify detailed BFD session information.

Action From operational mode, run the **show bfd session extensive** command for Device R0.

```
user@R0> show bfd session extensive
```

Address	State	Interface	Detect Time	Transmit Interval	Multiplier
192.168.0.1	Up	ge-2/0/0.0	0.030	0.010	3

Client L2CKT-OAM, TX interval 0.005, RX interval 0.010
 Session up time 03:47:14
 Local diagnostic None, remote diagnostic None
 Remote state Up, version 1
 Replicated
 Session type: VCCV BFD
 Min async interval 0.005, min slow interval 1.000
 Adaptive async TX interval 0.005, RX interval 0.010
 Local min TX interval 0.005, minimum RX interval 0.010, multiplier 3
 Remote min TX interval 0.005, min RX interval 0.010, multiplier 3
 Threshold transmission interval 0.030, Threshold for detection time 0.040
 Local discriminator 20, remote discriminator 13004
 Echo mode disabled/inactive
 Remote is control-plane independent
 Neighbor address 203.0.113.0, Virtual circuit id 1
 Session ID: 0x0

1 sessions, 1 clients
 Cumulative transmit rate 100.0 pps, cumulative receive rate 100.0 pps

Meaning The output shows detailed information for the BFD session.

Related Documentation

- [Configuring BFD for VCCV for Layer 2 Circuits on page 433](#)

Troubleshooting Layer 2 Circuits

- [Tracing Layer 2 Circuit Operations on page 443](#)

Tracing Layer 2 Circuit Operations

To trace the creation of and changes to Layer 2 circuits, include the **traceoptions** statement:

```
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 protocols l2circuit]**
- **[edit logical-systems *logical-system-name* protocols l2circuit]**

Specify the following flags to trace the indicated operations on Layer 2 circuits:

- **connections**—Layer 2 circuit connections (events and state changes)
- **error**—Error conditions
- **FEC**—Layer 2 circuit advertisements received or sent using LDP
- **topology**—Layer 2 circuit topology changes caused by reconfiguration or advertisements received from other PE routers

PART 6

Configuring VPWS VPNs

- [Overview on page 447](#)
- [Configuring VPWS VPNs on page 457](#)

CHAPTER 30

Overview

- [Understanding VPWS on page 447](#)
- [Supported VPWS Standards on page 450](#)
- [Understanding Multisegment Pseudowire for FEC 129 on page 451](#)

Understanding VPWS

Virtual private wire service (VPWS) Layer 2 VPNs employ Layer 2 services over MPLS to build a topology of point-to-point connections that connect end customer sites in a VPN. These Layer 2 VPNs provide an alternative to private networks that have been provisioned by means of dedicated leased lines or by means of Layer 2 virtual circuits that employ ATM or Frame Relay. The service provisioned with these Layer 2 VPNs is known as VPWS. You configure a VPWS *instance* on each associated edge device for each VPWS Layer 2 VPN.

Traditional VPNs over Layer 2 circuits require the provisioning and maintenance of separate networks for IP and for VPN services. In contrast, VPWS enables the sharing of a provider's core network infrastructure between IP and Layer 2 VPN services, reducing the cost of providing those services.

Junos OS supports two types of VPWS Layer 2 VPNs:

- Kompella Layer 2 VPNs, which use BGP for autodiscovery and signaling.
- FEC 129 BGP autodiscovery for VPWS, which uses BGP for autodiscovery and LDP as the signaling protocol.

FEC 129 BGP autodiscovery for VPWS requires the **l2vpn-id**, **source-attachment-identifier**, and **target-attachment-identifier** statements. Kompella Layer 2 VPNs require the **site-identifier** and **remote-site-id** statements.

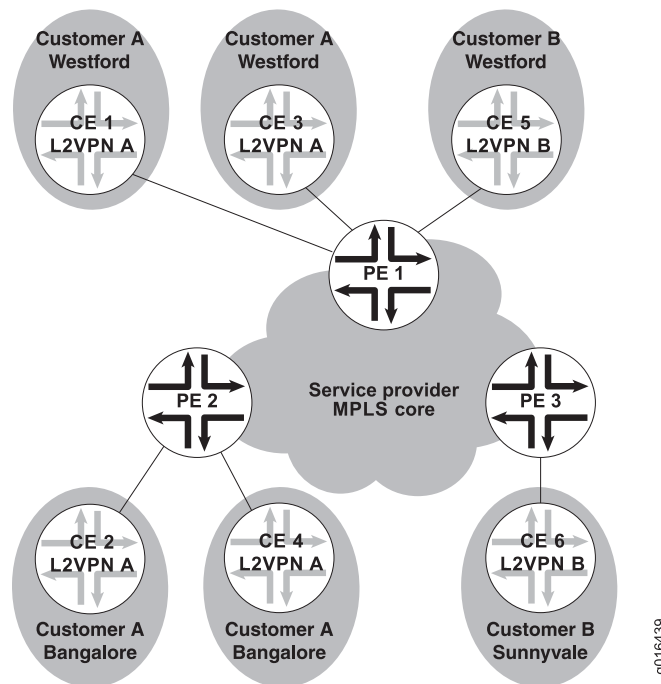


NOTE: VPWS creates pseudowires that emulate Layer 2 circuits. A virtual private LAN service (VPLS) network is similar to VPWS, but provides point-to-multipoint traffic forwarding in contrast to the VPWS Layer 2 VPN's point-to-point traffic forwarding. If you need point-to-multipoint service instead of point-to-point service, consider using VPLS instead of VPWS.

A VPWS Layer 2 VPN can have either a full-mesh or a hub-and-spoke topology. The tunneling mechanism in the core network typically is MPLS. However, VPWS can also use other tunneling protocols, such as GRE. VPWS is similar to Martini Layer 2 services over MPLS, and employs a similar encapsulation scheme for forwarding traffic.

Figure 39 on page 448 illustrates an example of a simple VPWS Layer 2 VPN topology.

Figure 39: VPWS Sample Topology



In this example, the service provider offers VPWS services to Customer A and Customer B. Customer A wants to create a full mesh of point-to-point links between Westford and Bangalore. Customer B needs only a single point-to-point link between Westford and Sunnyvale. The service provider uses BGP and MPLS signaling in the core, and creates a set of unidirectional pseudowires at each provider edge (PE) device to separately cross-connect each customer's Layer 2 circuits.

In order to provision this service, the provider configures two VPWS Layer 2 VPNs, Layer 2 VPN A and Layer 2 VPN B. The circuit cross-connect (CCC) encapsulation type (**ethernet-ccc** or **vlan-ccc**) is configured for each VPWS Layer 2 VPN. All interfaces in a given VPWS Layer 2 VPN must be configured with the VPWS Layer 2 VPN's encapsulation type.

Local and remote site information for the interfaces identifies the cross-connect. Local cross-connects are supported when the interfaces that are connected belong to two different sites configured in the same VPWS instance and on the same PE device.

BGP advertises reachability for the VPNs. The BGP configuration is similar to that used for other VPN services, such as Layer 3 VPNs and VPLS. MPLS is configured to set up base LSPs to the remote PE devices similarly to the other VPN services.

Junos OS provides VPWS support the following configuration methods:

- Pseudowires are manually configured using Forwarding Equivalence Class (FEC) 128.
- Pseudowires are signaled by LDP using FEC 129. This arrangement reduces the configuration burden that is associated with statically configured Layer 2 circuits while still using LDP as the underlying signaling protocol.

Supported and Unsupported Features

Junos OS supports the following features with VPWS :

- Intra-AS VPWS functionality using BGP for autodiscovery and FEC 129 LDP for pseudowire signaling.
- Graceful Routing Engine switchover.
- Operation, administration, and maintenance (OAM) mechanisms, including Bidirectional Forwarding Detection and MPLS ping.
- FEC 128 LDP signaling with static configuration (in Junos OS this is configured within **protocols l2circuit**). With this option, there is no BGP autodiscovery.

Junos OS does not support the following VPWS functionality:

- Multihoming of customer sites to multiple PE devices using the BGP site model of multihoming.
- Terminating FEC 129 VPWS into a mesh group of an FEC 129 VPLS instance.
- Intra-AS VPWS functionality using BGP for autodiscovery and FEC 128 LDP for pseudowire signaling.
- FEC 129 VPWS without BGP autodiscovery.
- Static configuration of VPWS with FEC 129 signaling.
- Nonstop active routing.
- Multi-segment pseudowires.
- Interworking of FEC 128 and FEC 129 VPWS.
- Statically configured Layer 2 circuit-style pseudowire redundancy.
- Inter-AS deployments.

Related Documentation

- [Example: Configuring BGP Autodiscovery for LDP VPLS on page 725](#)
- [Example: Configuring BGP Autodiscovery for LDP VPLS with User-Defined Mesh Groups on page 742](#)

Supported VPWS Standards

Junos OS substantially supports the following RFCs, which define standards for VPWS and Layer 2 circuits.

- RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*

Junos OS does not support Section 5.3, "The Generalized PWh FEC Element."

- RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*
- RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*
- RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*
- RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*

The following Internet drafts do not define standards, but provide information about Layer 2 technologies. The IETF classifies them as "Historic."

- Internet draft draft-martini-l2circuit-encap-mpls-11.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*

Junos OS differs from the Internet draft in the following ways:

- A packet with a sequence number of 0 (zero) is treated as out of sequence.
- Any packet that does not have the next incremental sequence number is considered out of sequence.
- When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.
- Internet draft draft-martini-l2circuit-trans-mpls-19.txt, *Transport of Layer 2 Frames Over MPLS*

Related Documentation

- [Supported Carrier-of-Carriers and Interprovider VPN Standards](#)
- [Supported Layer 2 VPN Standards on page 123](#)
- [Supported Layer 3 VPN Standards](#)
- [Supported Multicast VPN Standards](#)
- [Supported VPLS Standards on page 542](#)
- [Accessing Standards Documents on the Internet](#)

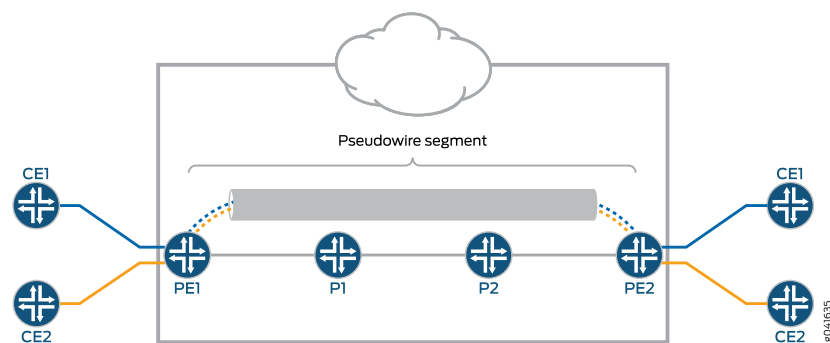
Understanding Multisegment Pseudowire for FEC 129

Understanding Multisegment Pseudowire

A pseudowire is a Layer 2 circuit or service that emulates the essential attributes of a telecommunications service, such as a T1 line, over an MPLS packet-switched network (PSN). The pseudowire is intended to provide only the minimum necessary functionality to emulate the wire with the required resiliency requirements for the given service definition.

When a pseudowire originates and terminates on the edge of the same PSN, the pseudowire label is unchanged between the originating and terminating provider edge (T-PE) devices. This is called a single-segment pseudowire (SS-PW). [Figure 40 on page 451](#) illustrates an SS-PW established between two PE routers. The pseudowires between the PE1 and PE2 routers are located within the same autonomous system (AS).

Figure 40: L2VPN Pseudowire

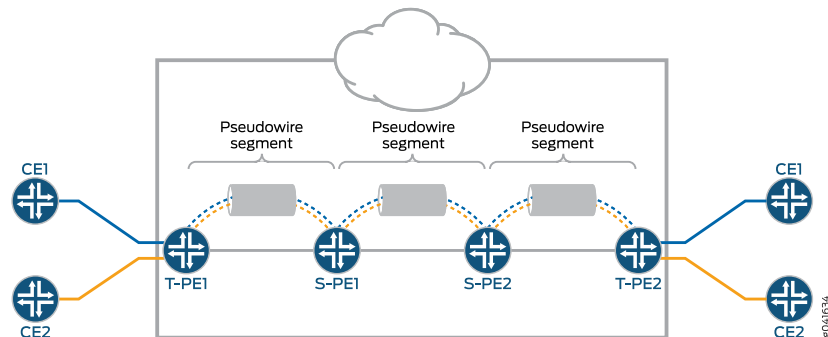


In cases where it is impossible to establish a single pseudowire from a local to a remote PE, either because it is unfeasible or undesirable to establish a single control plane between the two PEs, a multisegment pseudowire (MS-PW) is used.

An MS-PW is a set of two or more contiguous SS-PWs that are made to function as a single point-to-point pseudowire. It is also known as switched pseudowire. MS-PWs can go across different regions or network domains. A region can be considered as an interior gateway protocol (IGP) area or a BGP autonomous system that belongs to the same or different administrative domain. An MS-PW spans multiple cores or ASs of the same or different carrier networks. A Layer 2 VPN MS-PW can include up to 254 pseudowire segments.

[Figure 41 on page 452](#) illustrates a set of two or more pseudowire segments that function as a single pseudowire. The end routers are called terminating PE (T-PE) routers, and the switching routers are called switching PE (S-PE) routers. The S-PE router terminates the tunnels of the preceding and succeeding pseudowire segments in an MS-PW. The S-PE router can switch the control and data planes of the preceding and succeeding pseudowire segments of the MS-PW. An MS-PW is declared to be up when all the single-segment pseudowires are up.

Figure 41: Multisegment Pseudowire



Using FEC 129 for Multisegment Pseudowire

Currently, there are two types of attachment circuit identifiers (AII) defined under FEC 129:

- Type 1 AII
- Type 2 AII

The support of an MS-PW for FEC 129 uses type 2 AII. A type 2 AII is globally unique by definition of RFC 5003.

Single-segment pseudowires (SS-PWs) using FEC 129 on an MPLS PSN can use both type 1 and type 2 AII. For an MS-PW using FEC 129, a pseudowire itself is identified as a pair of endpoints. This requires that the pseudowire endpoints be uniquely identified.

In the case of a dynamically placed MS-PW, there is a requirement for the identifiers of attachment circuits to be globally unique, for the purposes of reachability and manageability of the pseudowire. Thus, individual globally unique addresses are allocated to all the attachment circuits and S-PEs that make up an MS-PW.

Type 2 AII is composed of three fields:

- Global_ID—Global identification, which is usually the AS number.
- Prefix—IPv4 address, which is usually the router ID.
- AC_ID—Local attachment circuit, which is a user-configurable value.

Since type 2 AII already contains the T-PE's IP address and it is globally unique, from the FEC 129 pseudowire signaling point of view, the combination (AGI, SAII, TAI) uniquely identifies an MS-PW across all interconnected pseudowire domains.

Establishing a Multisegment Pseudowire Overview

An MS-PW is established by dynamically and automatically selecting the predefined S-PEs and placing the MS-PW between two T-PE devices.

When S-PEs are dynamically selected, each S-PE is automatically discovered and selected using the BGP autodiscovery feature, without the requirement of provisioning the FEC

129 pseudowire-related information on all the S-PEs. BGP is used to propagate pseudowire address information throughout the PSN.

Since there is no manual provisioning of FEC 129 pseudowire information on the S-PEs, the Attachment Group Identifier (AGI) and Attachment Individual Identifier (AII) are reused automatically, and choosing the same set of S-PEs for the pseudowire in both the forwarding and reverse direction is achieved through the active and passive role of each T-PE device.

- **Active**—The T-PE initiates an LDP label mapping message.
- **Passive**—The T-PE does not initiate an LDP label mapping message until it receives a label mapping message initiated by the active T-PE. The passive T-PE sends its label mapping message to the same S-PE from where it received the label mapping message originated from its active T-PE. This ensures that the same set of S-PEs are used in the reverse direction.

Pseudowire Status Support for Multisegment Pseudowire

- [Pseudowire Status Behavior on T-PE on page 453](#)
- [Pseudowire Status Behavior on S-PE on page 453](#)

Pseudowire Status Behavior on T-PE

The following pseudowire status messages are relevant on the T-PE:

- 0x00000010—Local PSN-facing pseudowire (egress) transmit fault.
- 0x00000001—Generic nonforwarding fault code. This is set as the local fault code. The local fault code is set at the local T-PE, and LDP sends a pseudowire status TLV message with the same fault code to the remote T-PE.
- Fault codes are bit-wise OR'ed and stored as remote pseudowire status codes.

Pseudowire Status Behavior on S-PE

The S-PE initiates the pseudowire status messages that indicate the pseudowire faults. The SP-PE in the pseudowire notification message hints where the fault was originated.

- When a local fault is detected by the S-PE, a pseudowire status message is sent in both directions along the pseudowire. Since there are no attachment circuits on an S-PE, only the following status messages are relevant:
 - 0x00000008—Local PSN-facing pseudowire (ingress) receive fault.
 - 0x00000010—Local PSN-facing pseudowire (egress) transmit fault.
- To indicate which SS-PW is at fault, an LDP SP-PE TLV is attached with the pseudowire status code in the LDP notification message. The pseudowire status is passed along from one pseudowire to another unchanged by the control plane switching function.
- If an S-PE initiates a pseudowire status notification message with one particular pseudowire status bit, then for the pseudowire status code an S-PE receives, the same bit is processed locally and not forwarded until the S-PE's original status error is cleared.

- An S-PE keeps only two pseudowire status codes for each SS-PW it is involved in – local pseudowire status code and remote pseudowire status code. The value of the remote pseudowire status code is the result of logic or operation of the pseudowire status codes in the chain of SS-PWs preceding this segment. This status code is incrementally updated by each S-PE upon receipt and communicated to the next S-PE. The local pseudowire status is generated locally based on its local pseudowire status.
- Only transmit fault is detected at the SP-PE. When there is no MPLS LSP to reach the next segment, a local transmit fault is detected. The transmit fault is sent to the next downstream segment, and the receive fault is sent to the upstream segment.
- Remote failures received on an S-PE are just passed along the MS-PW unchanged. Local failures are sent to both segments of the pseudowire that the S-PE is involved in.

Pseudowire TLV Support for MS-PW

MS-PW provides the following support for the LDP SP-PE TLV [RFC 6073]:

- The LDP SP-PE TLVs for an MS-PW include:
 - Local IP address
 - Remote IP address
- An SP-PE adds the LDP SP-PE TLV to the label mapping message. Each SP-PE appends the local LDP SP-PE TLV to the SP-PE list it received from the other segment.
- The pseudowire status notification message includes the LDP SP-PE TLV when the notification is generated at the SP-PE.

Supported and Unsupported Features

Junos OS supports the following features with MS-PW:

- MPLS PSN for each SS-PW that builds up the MS-PW.
- The same pseudowire encapsulation for each SS-PW in an MS-PW – Ethernet or VLAN-CCC.
- The generalized PWid FEC with T-LDP as an end-to-end pseudowire signaling protocol to set up each SS-PW.
- MP-BGP to autodiscover the two endpoint PEs for each SS-PW associated with the MS-PW.
- Standard MPLS operation to stitch two side-by-side SS-PWs to form an MS-PW.
- Automatic discovery of S-PE so that the MS-PW can be dynamically placed.
- Minimum provisioning of S-PE.
- Operation, administration, and maintenance (OAM) mechanisms, including end-to-end MPLS ping or end-to-any-S-PE MPLS ping, MPLS path trace, end-to-end VCCV, and Bidirectional Forwarding Detection (BFD).
- Pseudowire swithing point (SP) PE TLV for the MS-PW.

- Composite next hop on MS-PW.
- Pseudowire status TLV for MS-PW.

Junos OS does not support the following MS-PW functionality:

- Mix of LDP FEC 128 and LDP FEC 129.
- Static pseudowire where each label is provisioned statically.
- Graceful Routing Engine switchover.
- Nonstop active routing.
- Multihoming.
- Partial connectivity verification (originating from an S-PE) in OAM.

**Related
Documentation**

- [Example: Configuring a Multisegment Pseudowire on page 492](#)
- [Example: Configuring FEC 129 BGP Autodiscovery for VPWS on page 708](#)

CHAPTER 31

Configuring VPWS VPNs

- [Understanding FEC 129 BGP Autodiscovery for VPWS on page 457](#)
- [Example: Configuring FEC 129 BGP Autodiscovery for VPWS on page 459](#)
- [Example: Configuring MPLS Egress Protection Service Mirroring for BGP Signaled Layer 2 Services on page 471](#)
- [Understanding Multisegment Pseudowire for FEC 129 on page 488](#)
- [Example: Configuring a Multisegment Pseudowire on page 492](#)
- [Configuring the FAT Flow Label for FEC 128 VPWS Pseudowires for Load-Balancing MPLS Traffic on page 534](#)
- [Configuring the FAT Flow Label for FEC 129 VPWS Pseudowires for Load-Balancing MPLS Traffic on page 536](#)

Understanding FEC 129 BGP Autodiscovery for VPWS

The major functional components in a VPWS with FEC 129 are BGP, LDP, and the Layer 2 VPN module of Junos OS. BGP is responsible for distributing the local autodiscovery routes created on each PE device to all other PE devices. LDP is responsible for using the autodiscovery information provided by BGP to set up targeted LDP sessions over which to signal the pseudowires. The Layer 2 VPN is the glue that binds the BGP and LDP functionalities together.

Supported Standards in FEC 129 BGP Autodiscovery for VPWS

The relevant RFCs for this feature are as follows:

- RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*
- RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*

Routes and Routing Table Interaction in FEC 129 BGP Autodiscovery for VPWS

BGP, LDP, and Layer 2 VPNs interact through different types of routes installed in the `instance.l2vpn.0` table. The routes that are present in the table are autodiscovery routes and pseudowire routes.

- Autodiscovery routes are used by BGP to allow autodiscovery of remote source access individual identifiers (SAIs) (the sources of the point-to-point pseudowires) and PE device addresses. Autodiscovery routes are advertised when you configure the **l2vpn auto-discovery-only** address family.

The format of the autodiscovery routes is a combination of the route distinguisher and the SAI. For example: 10.255.0.1:100:0.0.0.1/96 AD.

[Table 13 on page 458](#) lists the route elements and the number of associated bytes allocated to each element.

Table 13: Autodiscovery Route Format

Route Element	Bytes
RD	8 bytes
SAI	4 bytes

The **l2vpn-id** of the FEC 129 VPWS instance is attached to the route in a BGP extended community. One autodiscovery route is advertised for each source attachment identifier (SAI) in the instance.

- Pseudowire routes are installed by the Layer 2 VPN (local) and LDP (remote) to represent the bidirectional components of the pseudowire. For example: NoCtrlWord:5:100:200:2:0.0.0.1/176. The format of the routes is described in [Table 14 on page 458](#).

Table 14: Pseudowire Route Format

Field Name	Field Description
Pseudowire type + control word bit	2 bytes
Remote PE address	4 bytes
Attachment group identifier (AGI)	8 bytes
The AGI field of the pseudowire route is always set to the l2vpn-id of the instance.	
SAI	4 bytes
Target attachment individual identifier (TAII)	4 bytes

Layer 2 VPN Behavior in FEC 129 BGP Autodiscovery for VPWS

A Layer 2 VPN installs a locally generated autodiscovery route into the instance.l2vpn.0 table for every SAI configured in an FEC 129 VPWS instance. The extended community containing the **l2vpn-id** is attached when the route is added to the instance.l2vpn.0 table.

For each autodiscovered SAI from a remote neighbor where the **l2vpn-id** matches the local **l2vpn-id** and the received SAI matches a locally configured TAI, the Layer 2 VPN obtains an MPLS label and generates a pseudowire route and adds it to the

instance.l2vpn.0 table. The remote PE address is copied from the BGP protocol next hop for the autodiscovery route.

The Layer 2 VPN module of Junos OS is responsible for installing the forwarding routes into the mpls.0 table as usual.

BGP Autodiscovery Behavior in FEC 129 BGP Autodiscovery for VPWS

Local autodiscovery routes installed by the Layer 2 VPN in the instance.l2vpn.0 table are advertised by BGP to remote PE devices **sl2vpn auto-discovery-only** address family according to the instance and BGP export policies.

On the receiving side, BGP accepts autodiscovery routes from remote peers and installs them in the local bgp.l2vpn.0 table, if they are allowed by inbound policy. The route is installed, and a secondary route is imported into the instance.l2vpn.0 table when an import route target match between the route and instance is found.

LDP Signaling Behavior in VPWS in FEC 129 BGP Autodiscovery for VPWS

LDP listens for routes from instance.l2vpn.0 for any instance configured for FEC 129 VPWS. These routes are identified by the **instance-type l2vpn** statement in the routing instance and the presence of the **l2vpn-id** statement.

When a BGP autodiscovery route is installed, LDP sets up a targeted session with the remote peer, where the peer address is identified as the protocol next hop of the BGP autodiscovery route.

When a pseudowire route is installed in the instance.l2vpn.0 table, LDP uses the parameters associated with the route to signal the creation of the pseudowire using FEC 129. Upon receiving an FEC 129 label mapping message from a remote peer, LDP installs the pseudowire route in the ldp.l2vpn.0 table.

Upon a successful **l2vpn-id** match with a configured FEC 129 VPWS instance, a secondary pseudowire route is imported to the instance.l2vpn.0 table. If an outgoing pseudowire has not already been set up when the incoming pseudowire signaling is received, LDP initiates the outgoing pseudowire creation as well.

Related Documentation

- [Understanding VPWS on page 447](#)
- [Example: Configuring FEC 129 BGP Autodiscovery for VPWS on page 459](#)

Example: Configuring FEC 129 BGP Autodiscovery for VPWS

This example shows how to configure the virtual private wire service (VPWS), where remote provider edge (PE) devices are automatically discovered dynamically by BGP, and pseudowires are signaled by LDP using FEC 129. This arrangement reduces the configuration burden that is associated with statically configured Layer 2 circuits while still using LDP as the underlying signaling protocol.

- [Requirements on page 460](#)
- [Overview on page 460](#)

- [Configuration on page 464](#)
- [Verification on page 468](#)

Requirements

This example requires Junos OS Release 13.2 or later on the PE devices.

Overview

Because VPWS is a point-to-point service, FEC 129 VPWS routing instances are configured as **instance-type l2vpn**. As with FEC 129 VPLS, FEC 129 VPWS uses the **l2vpn-id** statement to define the Layer 2 VPN of which the routing instance is a member. The presence of the **l2vpn-id** statement designates that FEC 129 LDP signaling is used for the routing instance. The absence of **l2vpn-id** indicates that BGP signaling is used instead.

The point-to-point nature of VPWS requires that you specify the source access individual identifier (SAII) and the target access individual identifier (TAII). This SAII-TAII pair defines a unique pseudowire between two PE devices.

The SAII is specified with the **source-attachment-identifier** statement within the FEC 129 VPWS routing instance. You configure the source attachment identifier and the interfaces to associate with that source attachment identifier. Under each interface, you can configure the TAIL with the **target-attachment-identifier** statement. If the configured target identifier matches a source identifier advertised by a remote PE device by way of a BGP autodiscovery message, the pseudowire between that source-target pair is signaled. If there is no match between an advertised source identifier and the configured target identifier, the pseudowire is not established.

Sample: VPWS Configuration with Multiple Interfaces and Sites

```
routing-instances {
  FEC129-VPWS {
    instance-type l2vpn;
    interface ge-0/0/1.0;
    interface ge-0/0/2.0;
    interface ge-0/0/3.0;
    route-distinguisher 10.255.0.1:200;
    l2vpn-id l2vpn-id:100:200;
    vrf-target target:100:200;
    protocols l2vpn {
      site CUSTOMER-1 {
        source-attachment-identifier 1;
        interface ge-0/0/1.0 {
          target-attachment-identifier 2;
        }
        interface ge-0/0/2.0 {
          target-attachment-identifier 3;
        }
      }
    }
  }
}
```

You can configure multiple interfaces within a site, because each SAII-TAII pair defines a unique pseudowire, as shown with pseudowires 1-2 and 1-3 in the sample configuration. Both the source and target access identifiers are 4-byte numbers and can only be

configured in FEC 129 VPWS instances where the **instance-type** is **l2vpn** and the **l2vpn-id** configuration statement is present.

You can specify the source and target identifiers as plain unsigned integers in the range 1 through 4,292,967,295.

The Layer 2 circuit and Layer 2 VPN services allow many optional parameters to be included on a per-pseudowire basis. FEC 129 VPWS allows such parameters as MTU settings, community tagging, and inclusion of a control word, as shown in this sample configuration:

**Sample: VPWS
Configuration with
Optional Configuration
Parameters**

```
routing-instances {
  FEC129-VPWS {
    instance-type l2vpn;
    interface ge-0/0/1.0;
    interface ge-0/0/2.0;
    interface ge-0/0/3.0;
    route-distinguisher 10.255.0.1:200;
    l2vpn-id l2vpn-id:100:200;
    vrf-target target:100:200;
    protocols l2vpn {
      site CUSTOMER-1 {
        source-attachment-identifier 1;
        community COMM;
        control-word;
        encapsulation-type ethernet;
        ignore-encapsulation-mismatch;
        ignore-mtu-mismatch;
        mtu 1500;
        no-control-word;
        interface ge-0/0/1.0 {
          target-attachment-identifier 2;
        }
        interface ge-0/0/2.0 {
          target-attachment-identifier 3;
          community COMM;
          control-word;
          encapsulation-type ethernet;
          ignore-encapsulation-mismatch;
          ignore-mtu-mismatch;
          mtu 1500;
          no-control-word;
        }
      }
    }
  }
}
```

When configured within the site, the defined parameters affect any pseudowire originating from that site. When configured under an interface, the defined parameters affect that single specific pseudowire. This allows you to manipulate the parameters across all pseudowires associated with a particular local site in one place in the configuration.

Like other point-to-point services, the interfaces configured as members of the FEC 129 VPWS instance must be configured for CCC encapsulation and the CCC address family, as shown here:

```

interfaces {
  ge-0/0/1 {
    encapsulation ethernet-ccc;
    unit 0 {
      family ccc;
    }
  }
  ge-0/0/2 {
    encapsulation ethernet-ccc;
    unit 0 {
      family ccc;
    }
  }
  ge-0/0/3 {
    encapsulation ethernet-ccc;
    unit 0 {
      family ccc;
    }
  }
}

```

You can use **vlan-ccc** instead of **ethernet-ccc**.

To support the basic FEC 129 VPWS functionality, the BGP sessions on the PE devices also need to be configured with the BGP **auto-discovery-only** address family to allow exchange of the autodiscovery routes. If traditional BGP VPLS or Layer 2 VPN service is also provisioned on the PE devices, the address family **l2vpn signaling** is also required, as shown here:

```

bgp {
  group pe {
    type internal;
    local-address 10.255.0.1;
    family l2vpn {
      auto-discovery-only;
      signaling;
    }
    neighbor 10.255.0.2;
    neighbor 10.255.0.3;
  }
}

```

The following configuration sample shows an FEC 129 VPWS routing instance with the operation, administration, and maintenance (OAM) (ping and BFD) configuration options:

**Sample: VPWS
Configuration with
OAM**

```

routing-instances {
  FEC129-VPWS {
    instance-type l2vpn;
    interface ge-0/0/1.0;
    route-distinguisher 10.255.0.1:200;
    l2vpn-id l2vpn-id:100:200;
    vrf-target target:100:200;
  }
}

```

```

protocols l2vpn {
  oam {
    ping-interval 600;
    bfd-liveness-detection {
      minimum-interval 200;
    }
  }
  site CUSTOMER {
    source-attachment-identifier 1;
    oam {
      ping-interval 600;
      bfd-liveness-detection {
        minimum-interval 200;
      }
    }
  }
  interface ge-0/0/1.0 {
    oam {
      ping-interval 600;
      bfd-liveness-detection {
        minimum-interval 200;
      }
    }
    target-attachment-identifier 2;
  }
}
}
}

```

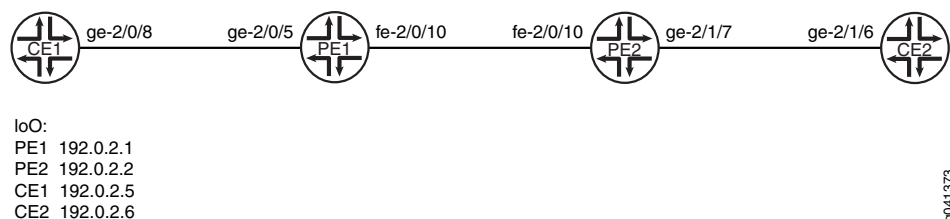
OAM options configured under **protocols l2vpn** apply to all sites and pseudowires in the routing instance. OAM options configured under a particular site apply to the pseudowires configured under that site. OAM options configured under a particular interface apply to the pseudowire configured under that interface.

Topology Diagram

Figure 42 on page 463 shows the topology used in this example.

This example uses a simple topology with two PE devices and two customer edge (CE) devices.

Figure 42: Simple VPWS Topology



“CLI Quick Configuration” on page 464 shows the configuration for all of the devices in Figure 42 on page 463. The section “Step-by-Step Procedure” on page 465 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	<pre>set interfaces ge-2/0/8 unit 0 description CE1_to_PE1 set interfaces ge-2/0/8 unit 0 family inet address 172.16.0.1/24 set interfaces lo0 unit 0 family inet address 192.0.2.5/24 set protocols ospf area 0.0.0.0 interface lo0.0 passive set protocols ospf area 0.0.0.0 interface ge-2/0/8.0</pre>
Device CE2	<pre>set interfaces ge-2/1/6 unit 0 description CE2_to_PE2 set interfaces ge-2/1/6 unit 0 family inet address 172.16.0.4/24 set interfaces lo0 unit 0 family inet address 192.0.2.6/24 set protocols ospf area 0.0.0.0 interface lo0.0 passive set protocols ospf area 0.0.0.0 interface ge-2/1/6.0</pre>
Device PE1	<pre>set interfaces ge-2/0/5 encapsulation ethernet-ccc set interfaces ge-2/0/5 unit 0 description PE1_to_CE1 set interfaces ge-2/0/5 unit 0 family ccc set interfaces fe-2/0/10 unit 0 description to_PE2 set interfaces fe-2/0/10 unit 0 family inet address 10.0.0.1/30 set interfaces fe-2/0/10 unit 0 family mpls set interfaces lo0 unit 0 family inet address 192.0.2.1/24 set protocols mpls interface fe-2/0/10.0 set protocols bgp local-address 192.0.2.1 set protocols bgp group pe-pe type internal set protocols bgp group pe-pe family l2vpn auto-discovery-only set protocols bgp group pe-pe family l2vpn signaling set protocols bgp group pe-pe neighbor 192.0.2.2 set protocols ospf traffic-engineering set protocols ospf area 0.0.0.0 interface lo0.0 passive set protocols ospf area 0.0.0.0 interface fe-2/0/10.0 set protocols ldp interface fe-2/0/10.0 set protocols ldp interface lo0.0 set routing-instances FEC129-VPWS instance-type l2vpn set routing-instances FEC129-VPWS interface ge-2/0/5.0 set routing-instances FEC129-VPWS route-distinguisher 192.0.2.1:100 set routing-instances FEC129-VPWS l2vpn-id l2vpn-id:100:100 set routing-instances FEC129-VPWS vrf-target target:100:100 set routing-instances FEC129-VPWS protocols l2vpn site ONE source-attachment-identifier 1 set routing-instances FEC129-VPWS protocols l2vpn site ONE interface ge-2/0/5.0 target-attachment-identifier 2 set routing-options autonomous-system 64510</pre>
Device PE2	<pre>set interfaces ge-2/1/7 encapsulation ethernet-ccc set interfaces ge-2/1/7 unit 0 description PE2_to_CE2 set interfaces ge-2/1/7 unit 0 family ccc set interfaces fe-2/0/10 unit 0 description to_PE1 set interfaces fe-2/0/10 unit 0 family inet address 10.0.0.2/30 set interfaces fe-2/0/10 unit 0 family mpls</pre>

```

set interfaces lo0 unit 0 family inet address 192.0.2.2/24
set protocols mpls interface fe-2/0/10.0
set protocols bgp local-address 192.0.2.2
set protocols bgp group pe-pe type internal
set protocols bgp group pe-pe family l2vpn auto-discovery-only
set protocols bgp group pe-pe family l2vpn signaling
set protocols bgp group pe-pe neighbor 192.0.2.1
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface fe-2/0/10.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ldp interface fe-2/0/10.0
set protocols ldp interface lo0.0
set routing-instances FEC129-VPWS instance-type l2vpn
set routing-instances FEC129-VPWS interface ge-2/1/7.0
set routing-instances FEC129-VPWS route-distinguisher 192.0.2.2:100
set routing-instances FEC129-VPWS l2vpn-id l2vpn-id:100:100
set routing-instances FEC129-VPWS vrf-target target:100:100
set routing-instances FEC129-VPWS protocols l2vpn site TWO
    source-attachment-identifier 2
set routing-instances FEC129-VPWS protocols l2vpn site TWO interface ge-2/1/7.0
    target-attachment-identifier 1
set routing-options autonomous-system 64510

```

Step-by-Step Procedure

To configure a FEC 129 VPWS:

1. Configure the interfaces.

```
[edit interfaces]
```

```

user@PE1# set ge-2/0/5 encapsulation ethernet-ccc
user@PE1# set ge-2/0/5 unit 0 description PE1_to_CE1
user@PE1# set ge-2/0/5 unit 0 family ccc

```

```

user@PE1# set fe-2/0/10 unit 0 description to_PE2
user@PE1# set fe-2/0/10 unit 0 family inet address 10.0.0.1/30
user@PE1# set fe-2/0/10 unit 0 family mpls

```

```
user@PE1# set lo0 unit 0 family inet address 192.0.2.1/24
```

2. Configure MPLS on the core-facing interface.

```
[edit protocols mpls]
```

```
user@PE1# set interface fe-2/0/10.0
```

3. Configure BGP.

```
[edit protocols bgp]
```

```

user@PE1# set local-address 192.0.2.1
user@PE1# set group pe-pe type internal
user@PE1# set group pe-pe family l2vpn auto-discovery-only
user@PE1# set group pe-pe family l2vpn signaling
user@PE1# set group pe-pe neighbor 192.0.2.2

```

4. Configure an interior gateway protocol, such as IS-IS or OSPF.

If you use OSPF, enable traffic engineering. Traffic engineering is supported by IS-IS by default.

```
[edit protocols ospf]
user@PE1# set traffic-engineering
user@PE1# set area 0.0.0.0 interface lo0.0 passive
user@PE1# set area 0.0.0.0 interface fe-2/0/10.0
```

5. Configure LDP on the core-facing interface and on the loopback interface.

```
[edit protocols ldp]
user@PE1# set interface fe-2/0/10.0
user@PE1# set interface lo0.0
```

6. Configure the VPWS routing instance.

LDP listens for routes from instance.l2vpn.0 for any instance configured for FEC 129 VPWS. These routes are identified by the **instance-type l2vpn** statement in the routing instance and the presence of the **l2vpn-id** statement.

Make sure that the **target-attachment-identifier** matches the **source-attachment-identifier** in the remote PE device's corresponding site. In this example, the pseudowire is established between Device PE1 and Device PE2. Device PE1 uses SAI 1 and TAI 2, while Device PE2 uses the opposite, SAI 2 and TAI 1.

```
[edit routing-instances FEC129-VPWS]
user@PE1# set instance-type l2vpn
user@PE1# set interface ge-2/0/5.0
user@PE1# set route-distinguisher 192.0.2.1:100
user@PE1# set l2vpn-id l2vpn-id:100:100
user@PE1# set vrf-target target:100:100
user@PE1# set protocols l2vpn site ONE source-attachment-identifier 1
user@PE1# set protocols l2vpn site ONE interface ge-2/0/5.0
target-attachment-identifier 2
```

7. Configure the autonomous system (AS) number.

```
[edit routing-options]
user@PE1# set autonomous-system 64510
```

8. If you are done configuring the device, commit the configuration.

```
[edit]
user@PE1# commit
```

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

```
user@PE1# show interfaces
ge-2/0/5 {
  encapsulation ethernet-ccc;
  unit 0 {
    description PE1_to_CE1;
    family ccc;
```

```

    }
  }
  fe-2/0/10 {
    unit 1 {
      description to_PE2;
      family inet {
        address 10.0.0.1/30;
      }
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 192.0.2.1/24;
      }
    }
  }
}

user@PE1# show protocols
mpls {
  interface fe-2/0/10.0;
}
bgp {
  local-address 192.0.2.1;
  group pe-pe {
    type internal;
    family l2vpn {
      auto-discovery-only;
      inactive: signaling;
    }
    neighbor 192.0.2.2;
  }
}
ospf {
  traffic-engineering;
  area 0.0.0.0 {
    interface lo0.0 {
      passive;
    }
    interface fe-2/0/10.0;
  }
}
ldp {
  interface fe-2/0/10.0;
  interface lo0.0;
}

user@PE1# show routing-instances
FEC129-VPWS {
  instance-type l2vpn;
  interface ge-2/0/5.0;
  route-distinguisher 192.0.2.1:100;
  l2vpn-id l2vpn-id:100:100;
  vrf-target target:100:100;
  protocols {
    l2vpn {

```

```

site ONE {
    source-attachment-identifier 1;
    interface ge-2/0/5.0 {
        target-attachment-identifier 2;
    }
}
}
}
}

user@PE1# show routing-options
autonomous-system 64510;

```

Verification

Confirm that the configuration is working properly.

- [Verifying the Routes on page 468](#)
- [Checking Connectivity Between the CE Devices on page 469](#)
- [Checking the VPWS Connections on page 470](#)
- [Checking Connectivity Between the PE Devices on page 471](#)

Verifying the Routes

Purpose Verify that the expected routes are learned.

Action From operational mode, enter the **show route** command.

```

user@PE1> show route
inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.1/24          *[Direct/0] 6d 21:16:32
> via lo0.0
192.0.2.2/24          *[OSPF/10] 6d 21:15:31, metric 1
> to 10.0.0.2 via fe-2/0/10.0
10.0.0.0/30           *[Direct/0] 6d 21:16:31
> via fe-2/0/10.0
10.0.0.1/32           *[Local/0] 6d 21:16:32
Local via fe-2/0/10.0
203.0.113.0/24        *[OSPF/10] 6d 21:16:34, metric 1
MultiRecv

inet.3: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.2/24          *[LDP/9] 5d 22:25:19, metric 1
> to 10.0.0.2 via fe-2/0/10.0

mpls.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0                    *[MPLS/0] 6d 21:16:33, metric 1
Receive
1                    *[MPLS/0] 6d 21:16:33, metric 1
Receive
2                    *[MPLS/0] 6d 21:16:33, metric 1

```



```

13          Receive
          *[MPLS/0] 6d 21:16:33, metric 1
          Receive
299808      *[LDP/9] 5d 22:25:19, metric 1
            > to 10.0.0.2 via fe-2/0/10.0, Pop
299808(S=0) *[LDP/9] 5d 22:25:19, metric 1
            > to 10.0.0.2 via fe-2/0/10.0, Pop
299824      *[L2VPN/7] 5d 22:25:18
            > via ge-2/0/5.0, Pop
ge-2/0/5.0  *[L2VPN/7] 5d 22:13:02, metric2 1
            > to 10.0.0.2 via fe-2/0/10.0, Push 299872

bgp.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.2:100:0.0.0.2/96 AD
          *[BGP/170] 6d 20:51:23, localpref 100, from 192.0.2.2
          AS path: I, validation-state: unverified
          > to 10.0.0.2 via fe-2/0/10.0

ldp.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.2:NoCtrlWord:5:100:100:0.0.0.2:0.0.0.1/176
          *[LDP/9] 5d 22:13:02
          Discard

FEC129-VPWS.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.1:100:0.0.0.1/96 AD
          *[L2VPN/170] 6d 20:53:26, metric2 1
          Indirect
192.0.2.2:100:0.0.0.2/96 AD
          *[BGP/170] 6d 20:51:23, localpref 100, from 192.0.2.2
          AS path: I, validation-state: unverified
          > to 10.0.0.2 via fe-2/0/10.0
192.0.2.2:NoCtrlWord:5:100:100:0.0.0.1:0.0.0.2/176
          *[L2VPN/7] 6d 20:51:23, metric2 1
          > to 10.0.0.2 via fe-2/0/10.0
192.0.2.2:NoCtrlWord:5:100:100:0.0.0.2:0.0.0.1/176
          *[LDP/9] 5d 22:13:02
          Discard

```

Meaning The output shows all the learned routes, including the autodiscovery (AD) routes.

Checking Connectivity Between the CE Devices

Purpose Verify that Device CE1 can ping Device CE2.

Action user@CE1> ping 192.0.2.6
 PING 192.0.2.6 (192.0.2.6): 56 data bytes
 64 bytes from 192.0.2.6: icmp_seq=0 ttl=64 time=0.679 ms
 64 bytes from 192.0.2.6: icmp_seq=1 ttl=64 time=0.524 ms
 ^C
 --- 192.0.2.6 ping statistics ---
 2 packets transmitted, 2 packets received, 0% packet loss
 round-trip min/avg/max/stddev = 0.524/0.602/0.679/0.078 ms

Meaning The output shows that the VPWS is operational.

Checking the VPWS Connections

Purpose Make sure that all of the FEC 129 VPWS connections come up correctly.

Action user@PE1> show l2vpn connections
 Layer-2 VPN connections:

Legend for connection status (St)
 EI -- encapsulation invalid NC -- interface encapsulation not CCC/TCC/VPLS
 EM -- encapsulation mismatch WE -- interface and instance encaps not same
 VC-Dn -- Virtual circuit down NP -- interface hardware not present
 CM -- control-word mismatch -> -- only outbound connection is up
 CN -- circuit not provisioned <- -- only inbound connection is up
 OR -- out of range Up -- operational
 OL -- no outgoing label Dn -- down
 LD -- local site signaled down CF -- call admission control failure
 RD -- remote site signaled down SC -- local and remote site ID collision
 LN -- local site not designated LM -- local site ID not minimum designated
 RN -- remote site not designated RM -- remote site ID not minimum designated
 XX -- unknown connection status IL -- no incoming label
 MM -- MTU mismatch MI -- Mesh-Group ID not available
 BK -- Backup connection ST -- Standby connection
 PF -- Profile parse failure PB -- Profile busy
 RS -- remote site standby SN -- Static Neighbor
 LB -- Local site not best-site RB -- Remote site not best-site
 VM -- VLAN ID mismatch

Legend for interface status
 Up -- operational
 Dn -- down

Instance: FEC129-VPWS
 L2vpn-id: 100:100
Local source-attachment-id: 1 (ONE)

Target-attachment-id	Type	St	Time last up	# Up trans
2	rmt	Up	Nov 28 16:16:14 2012	1

Remote PE: 192.0.2.2, Negotiated control-word: No
 Incoming label: 299792, Outgoing label: 299792
 Local interface: ge-2/0/5.0, Status: Up, Encapsulation: ETHERNET

Meaning As expected, the connection is up. The output includes the source attachment ID and the target attachment ID.

Checking Connectivity Between the PE Devices

Purpose	Verify that Device PE1 can ping Device PE2. The <code>ping mpls l2vpn fec129</code> command accepts SAs and TAs as integers or IP addresses and also allows you to use the CE-facing interface instead of the other parameters (<code>instance</code> , <code>local-id</code> , <code>remote-id</code> , <code>remote-pe-address</code>).
Action	<pre> user@PE1> ping mpls l2vpn fec129 instance FEC129-VPWS remote-id 2 remote-pe-address 192.0.2.2 local-id 1 !!!! --- lsping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss user@PE1> ping mpls l2vpn fec129 interface ge-2/0/5.0 !!!! --- lsping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss </pre>
Meaning	The output shows that the VPWS is operational.
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring BGP Autodiscovery for LDP VPLS on page 725 • Example: Configuring BGP Autodiscovery for LDP VPLS with User-Defined Mesh Groups on page 742

Example: Configuring MPLS Egress Protection Service Mirroring for BGP Signaled Layer 2 Services

If there is a link or node failure in the core network, a protection mechanism such as MPLS fast reroute can be triggered on the transport LSPs between the PE routers to repair the connection within tens of milliseconds. An egress protection LSP addresses the problem of a node-link failure at the edge of the network (for example, a failure of a PE router).

This example shows how to configure link protection for BGP signaled Layer 2 services.

- [Requirements on page 471](#)
- [Overview on page 471](#)
- [Configuration on page 473](#)
- [Verification on page 485](#)

Requirements

MX Series Routers running Junos OS Release 14.2 or later.

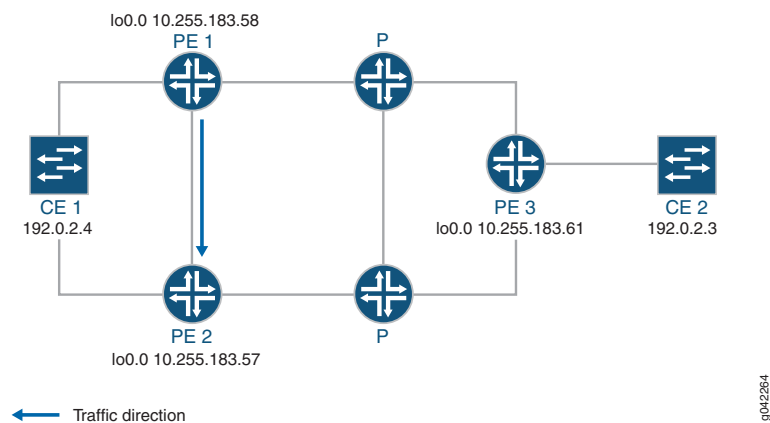
Overview

If there is a link or node failure in the core network, a protection mechanism such as MPLS fast reroute can be triggered on the transport LSPs between the PE routers to repair the connection within tens of milliseconds. An egress protection LSP addresses the problem of a node-link failure at the edge of the network (for example, a failure of a PE router).

This example includes the following configuration concepts and statements that are unique to the configuration of an egress protection LSP:

- **context-identifier**—Specifies an IPv4 or IPv6 address used to define the pair of PE routers participating in the egress protection LSP. It is assigned to each ordered pair of primary PE and the protector to facilitate protection establishment. This address is globally unique, or unique in the address space of the network where the primary PE and the protector reside.
- **egress-protection**—Configures the protector information for the protected Layer 2 circuit and configures the protector Layer 2 circuit at the **[edit protocols mpls]** hierarchy level. Configures an LSP as an egress protection LSP at the **[edit protocols mpls]** hierarchy level.
- **protector**—Configures the creation of standby pseudowires on the backup PE for link or node protection for the instance.

Figure 43: Egress Protection LSP Configured from Router PE1 to Router PE2



In the event of a failure of the egress PE Router PE1, traffic is switched to the egress protection LSP configured between Router PE1 and Router PE2 (the protector PE router):

- Device CE2—Traffic origin
- Router PE3—Ingress PE router
- Router PE1— (Primary) Egress PE router
- Router PE2—Protector PE router
- Device CE1—Traffic destination

When the link between CE1– PE1 goes down, PE1 will briefly redirect that traffic toward CE1, to PE2. PE2 forwards it to CE1 until ingress router PE3 recalculates to forward the traffic to PE2.

Initially the traffic direction was: CE2 – PE3 – P – PE1 – CE1.

When the link between CE1– PE1 goes down, the traffic will be: CE2 – PE3 – P – PE1 – PE2 – CE1. PE3 then recalculates the path: CE2 – PE3 – P – PE2 – CE1.

This example shows how to configure routers PE1, PE2, and PE3.

Configuration

- [Step-by-Step Procedure on page 475](#)
- [Results on page 479](#)

CLI Quick Configuration

To quickly configure an egress protection LSP, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configurations, copy and then paste the commands into the CLI and enter **commit** from configuration mode.

PE1

```

set protocols rsvp interface all
set protocols rsvp interface fxp0.0 disable
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols mpls egress-protection context-identifier 203.0.113.1 primary
set protocols mpls egress-protection context-identifier 203.0.113.1 advertise-mode
  stub-alias
set protocols mpls egress-protection traceoptions file ep size 100m
set protocols mpls egress-protection traceoptions flag all
set protocols bgp traceoptions file bgp.log world-readable
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 10.255.183.58
set protocols bgp group ibgp family inet unicast
set protocols bgp group ibgp family l2vpn signaling egress-protection
set protocols bgp group ibgp neighbor 192.0.2.3
set protocols bgp group ibgp neighbor 192.0.2.4
set protocols isis traceoptions file isis-edge size 10m world-readable
set protocols isis traceoptions flag error
set protocols isis level 1 disable
set protocols isis level 2 wide-metrics-only
set protocols isis interface all point-to-point
set protocols isis interface all level 2 metric 10
set protocols isis interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set policy-options policy-statement lb then load-balance per-packet
set routing-options traceoptions file ro.log
set routing-options traceoptions flag all
set routing-options traceoptions flag route
set routing-options autonomous-system 100
set routing-options forwarding-table export lb
set routing-instances foo instance-type l2vpn
set routing-instances foo egress-protection context-identifier 203.0.113.1
set routing-instances foo interface ge-2/0/2.0
set routing-instances foo route-distinguisher 10.255.183.58:1
set routing-instances foo vrf-target target:9000:1
set routing-instances foo protocols l2vpn encapsulation-type ethernet-vlan
set routing-instances foo protocols l2vpn site foo site-identifier 1

```

```
set routing-instances foo protocols l2vpn site foo multi-homing
set routing-instances foo protocols l2vpn site foo site-preference primary
set routing-instances foo protocols l2vpn site foo interface ge-2/0/2.0 remote-site-id 2
```

PE2

```
set protocols rsvp interface all
set protocols rsvp interface fxp0.0 disable
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols mpls egress-protection context-identifier 203.0.113.1 protector
set protocols mpls egress-protection context-identifier 203.0.113.1 advertise-mode
  stub-alias
set protocols mpls egress-protection traceoptions file ep size 100m
set protocols mpls egress-protection traceoptions flag all
set protocols bgp traceoptions file bgp.log world-readable
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 10.255.183.57
set protocols bgp group ibgp family inet unicast
set protocols bgp group ibgp family l2vpn signaling egress-protection
set protocols bgp group ibgp neighbor 192.0.2.3
set protocols bgp group ibgp neighbor 192.0.2.4
set protocols isis traceoptions file isis-edge size 10m world-readable
set protocols isis traceoptions flag error
set protocols isis level 1 disable
set protocols isis level 2 wide-metrics-only
set protocols isis interface all point-to-point
set protocols isis interface all level 2 metric 10
set protocols isis interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set policy-options policy-statement lb then load-balance per-packet
set routing-options traceoptions file ro.log
set routing-options traceoptions flag normal
set routing-options traceoptions flag route
set routing-options autonomous-system 100
set routing-options forwarding-table export lb
set routing-instances foo instance-type l2vpn
set routing-instances foo egress-protection protector
set routing-instances foo interface ge-2/0/2.0
set routing-instances foo route-distinguisher 10.255.183.57:1
set routing-instances foo vrf-target target:9000:1
set routing-instances foo protocols l2vpn encapsulation-type ethernet-vlan
set routing-instances foo protocols l2vpn site foo hot-standby
set routing-instances foo protocols l2vpn site foo site-identifier 1
set routing-instances foo protocols l2vpn site foo multi-homing
set routing-instances foo protocols l2vpn site foo site-preference backup
set routing-instances foo protocols l2vpn site foo interface ge-2/0/2.0 remote-site-id 2
```

PE3

```
set protocols rsvp interface all
set protocols rsvp interface fxp0.0 disable
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols bgp traceoptions file bgp.log world-readable
set protocols bgp group ibgp type internal
```

```

set protocols bgp group ibgp local-address 10.255.183.61
set protocols bgp group ibgp family inet unicast
set protocols bgp group ibgp family l2vpn signaling
set protocols bgp group ibgp neighbor 192.0.2.3
set protocols bgp group ibgp neighbor 192.0.2.4
set protocols isis traceoptions file isis-edge size 10m world-readable
set protocols isis traceoptions flag error
set protocols isis level 1 disable
set protocols isis level 2 wide-metrics-only
set protocols isis interface all point-to-point
set protocols isis interface all level 2 metric 10
set protocols isis interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set policy-options policy-statement lb then load-balance per-packet
set routing-options traceoptions file ro.log
set routing-options traceoptions flag normal
set routing-options traceoptions flag route
set routing-options autonomous-system 100
set routing-options forwarding-table export lb
set routing-instances foo instance-type l2vpn
set routing-instances foo interface ge-2/1/2.0
set routing-instances foo route-distinguisher 10.255.183.61:1
set routing-instances foo vrf-target target:9000:1
set routing-instances foo protocols l2vpn encapsulation-type ethernet-vlan
set routing-instances foo protocols l2vpn site foo site-identifier 2
set routing-instances foo protocols l2vpn site foo interface ge-2/1/2.0 remote-site-id 1

```

Step-by-Step Procedure

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 an egress protection LSP for router PE1:

1. Configure RSVP.


```

[edit protocols rsvp]
user@PE1# set interface all
user@PE1# set interface fxp0.0 disable

```
2. Configure MPLS to use the egress protection LSP to protect against a link failure to Device CE1.


```

[edit protocols mpls]
user@PE1# set interface all
user@PE1# set interface fxp0.0 disable
user@PE1# set egress-protection context-identifier 203.0.113.1 primary
user@PE1# set egress-protection context-identifier 203.0.113.1 advertise-mode stub-alias
user@PE1# set egress-protection traceoptions file ep size 100m
user@PE1# set egress-protection traceoptions flag all

```
3. Configure BGP.


```

[edit protocols bgp]

```

```
user@PE1# set traceoptions file bgp.log world-readable
user@PE1# set group ibgp type internal
user@PE1# set group ibgp local-address 10.255.183.58
user@PE1# set group ibgp family inet unicast
user@PE1# set group ibgp family l2vpn signaling egress-protection
user@PE1# set group ibgp neighbor 192.0.2.3
user@PE1# set group ibgp neighbor 192.0.2.4
```

4. Configure IS-IS.

```
[edit protocols isis]
user@PE1# set traceoptions file isis-edge size 10m world-readable
user@PE1# set traceoptions flag error
user@PE1# set level 1 disable
user@PE1# set level 2 wide-metrics-only
user@PE1# set interface all point-to-point
user@PE1# set interface all level 2 metric 10
user@PE1# set interface fxp0.0 disable
```

5. Configure LDP.

```
[edit protocols ldp]
user@PE1# set interface all
user@PE1# set interface fxp0.0 disable
```

6. Configure a load-balancing policy.

```
[edit]
user@PE1# set policy-options policy-statement lb then load-balance per-packet
```

7. Configure the routing options to export routes based on the load-balancing policy.

```
[edit routing-options]
user@PE1# set traceoptions file ro.log
user@PE1# set traceoptions flag all
user@PE1# set autonomous-system 100
user@PE1# set forwarding-table export lb
```

8. Configure BGP to advertise NRL1 from the routing instance with context-ID as next-hop.

```
[edit routing-instances]
user@PE1# set foo instance-type l2vpn
user@PE1# set foo egress-protection context-identifier 203.0.113.1
user@PE1# set foo interface ge-2/0/2.0
user@PE1# set foo route-distinguisher 10.255.183.58:1
user@PE1# set foo vrf-target target:9000:1
```

9. Configure l2vpn instance to use the egress LSP configured.

```
[edit routing-instances]
user@PE1# set foo protocols l2vpn encapsulation-type ethernet-vlan
user@PE1# set foo protocols l2vpn site foo site-identifier 1
user@PE1# set foo protocols l2vpn site foo multi-homing
user@PE1# set foo protocols l2vpn site foo site-preference primary
user@PE1# set foo protocols l2vpn site foo interface ge-2/0/2.0 remote-site-id 2
```

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

**Step-by-Step
Procedure**

To configure an egress protection LSP for Router PE2:

1. Configure RSVP.


```
[edit protocols rsvp]
user@PE2# set interface all
user@PE2# set interface fxp0.0 disable
```
2. Configure MPLS and the LSP that acts as the egress protection LSP.


```
[edit protocols mpls]
user@PE2# set interface all
user@PE2# set interface fxp0.0 disable
user@PE2# set egress-protection context-identifier 203.0.113.1 protector
user@PE2# set egress-protection context-identifier 203.0.113.1 advertise-mode
stub-alias
user@PE2# set egress-protection traceoptions file ep size 100m
user@PE2# set egress-protection traceoptions flag all
```
3. Configure BGP.


```
[edit protocols bgp]
user@PE2# set traceoptions file bgp.log world-readable
user@PE2# set group ibgp type internal
user@PE2# set group ibgp local-address 10.255.183.57
user@PE2# set group ibgp family inet unicast
user@PE2# set group ibgp family l2vpn signaling
user@PE2# set group ibgp family l2vpn egress-protection
user@PE2# set group ibgp neighbor 192.0.2.3
user@PE2# set group ibgp neighbor 192.0.2.4
```
4. Configure IS-IS.


```
[edit protocols isis]
user@PE2# set traceoptions file isis-edge size 10m world-readable
user@PE2# set traceoptions flag error
user@PE2# set level 1 disable
user@PE2# set level 2 wide-metrics-only
user@PE2# set interface all point-to-point
user@PE2# set interface all level 2 metric 10
user@PE2# set interface fxp0.0 disable
```
5. Configure LDP.


```
[edit protocols ldp]
user@PE2# set interface all
user@PE2# set interface fxp0.0 disable
```
6. Configure a load-balancing policy.


```
[edit]
user@PE2# set policy-options policy-statement lb then load-balance per-packet
```
7. Configure the routing options to export routes based on the load-balancing policy.


```
[edit routing-options]
user@PE2# set traceoptions file ro.log
user@PE2# set traceoptions flag all
user@PE2# set autonomous-system 100
user@PE2# set forwarding-table export lb
```

8. Configure BGP to advertise NRLI from the routing instance with context-ID as next-hop.

```
[edit routing-instances]
user@PE2# set foo instance-type l2vpn
user@PE2# set foo egress-protection protector
user@PE2# set foo interface ge-2/0/2.0
user@PE2# set foo route-distinguisher 10.255.183.57:1
user@PE2# set foo vrf-target target:9000:1
```

9. Configure l2vpn instance to use the egress LSP configured.

```
[edit routing-instances]
user@PE2# set foo protocols l2vpn encapsulation-type ethernet-vlan
user@PE2# set foo protocols l2vpn site foo hot-standby
user@PE2# set foo protocols l2vpn site foo site-identifier 1
user@PE2# set foo protocols l2vpn site foo multi-homing
user@PE2# set foo protocols l2vpn site foo site-preference backup
user@PE2# set foo protocols l2vpn site foo interface ge-2/0/2.0 remote-site-id 2
```

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

Step-by-Step Procedure

To configure an egress protection LSP for Router PE3:

1. Configure RSVP.

```
[edit protocols rsvp]
user@PE3# set interface all
user@PE3# set interface fxp0.0 disable
```

2. Configure MPLS.

```
[edit protocols mpls]
user@PE3# set interface all
user@PE3# set interface fxp0.0 disable
```

3. Configure BGP.

```
[edit protocols bgp]
user@PE3# set traceoptions file bgp.log world-readable
user@PE3# set group ibgp type internal
user@PE3# set group ibgp local-address 10.255.183.61
user@PE3# set group ibgp family inet unicast
user@PE3# set group ibgp family l2vpn signaling
user@PE3# set group ibgp neighbor 192.0.2.3
user@PE3# set group ibgp neighbor 192.0.2.4
```

4. Configure IS-IS.

```
[edit protocols isis]
user@PE3# set traceoptions file isis-edge size 10m world-readable
user@PE3# set traceoptions flag error
user@PE3# set level 1 disable
user@PE3# set level 2 wide-metrics-only
user@PE3# set protocols isis interface all point-to-point
[edit protocols isis]
user@PE3# set protocols isis interface all level 2 metric 10
[edit protocols isis]
user@PE3# set protocols isis interface fxp0.0 disable
```

5. Configure LDP.


```
[edit protocols ldp]
user@PE3# set interface all
user@PE3# set interface fxp0.0 disable
```
6. Configure a load-balancing policy.


```
[edit]
user@PE3# set policy-options policy-statement lb then load-balance per-packet
```
7. Configure the routing options to export routes based on the load-balancing policy.


```
[edit routing-options]
user@PE3# set traceoptions file ro.log
user@PE3# set traceoptions flag normal
user@PE3# set traceoptions flag route
user@PE3# set autonomous-system 100
user@PE3# set forwarding-table export lb
```
8. Configure BGP to advertise NRLI from the routing instance with context-ID as next-hop.


```
[edit]
user@PE3# set routing-instances foo instance-type l2vpn
user@PE3# set routing-instances foo interface ge-2/1/2.0
user@PE3# set routing-instances foo route-distinguisher 10.255.183.61:1
user@PE3# set routing-instances foo vrf-target target:9000:1
```
9. Configure l2vpn to specify the interface that connects to the site and the remote interface to which you want the specified interface to connect.


```
[edit routing-instances]
user@PE3# set foo protocols l2vpn encapsulation-type ethernet-vlan
user@PE3# set foo protocols l2vpn site foo site-identifier 2
user@PE3# set foo protocols l2vpn site foo interface ge-2/1/2.0 remote-site-id 1
```
10. If you are done configuring the device, enter **commit** from configuration.

Results

From configuration mode, confirm your configuration on Router PE1 by entering the **show protocols**, **show policy-options**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@PE1# show protocols
rsvp {
  interface all;
  interface fxp0.0 {
    disable;
  }
}
mpls {
  interface all;
  interface fxp0.0 {
    disable;
```

```
}
  egress-protection {
    context-identifier 203.0.113.1 {
      primary;
      advertise-mode stub-alias;
    }
    traceoptions {
      file ep size 100m;
      flag all;
    }
  }
}
bgp {
  traceoptions {
    file bgp.log world-readable;
  }
  group ibgp {
    type internal;
    local-address 10.255.183.58;
    family inet {
      unicast;
    }
    family l2vpn {
      signaling {
        egress-protection;
      }
    }
    neighbor 192.0.2.3;
    neighbor 192.0.2.4;
  }
}
isis {
  traceoptions {
    file isis-edge size 10m world-readable;
    flag error;
  }
  level 1 disable;
  level 2 wide-metrics-only;
  interface all {
    point-to-point;
    level 2 metric 10;
  }
  interface fxp0.0 {
    disable;
  }
}
ldp {
  interface all;
  interface fxp0.0 {
    disable;
  }
}
```

```
[edit]
user@PE1# show policy-options
```

```

policy-statement lb {
  then {
    load-balance per-packet;
  }
}
[edit]
user@PE1# show routing-options
traceoptions {
  file ro.log;
  flag all;
}
autonomous-system 100;
forwarding-table {
  export lb;
}

[edit]
user@PE1# show routing-instances
foo {
  instance-type l2vpn;
  egress-protection {
    context-identifier {
      203.0.113.1;
    }
  }
  interface ge-2/0/2.0;
  route-distinguisher 10.255.183.58:1;
  vrf-target target:9000:1;
  protocols {
    l2vpn {
      encapsulation-type ethernet-vlan;
      site foo {
        site-identifier 1;
        multi-homing;
        site-preference primary;
        interface ge-2/0/2.0 {
          remote-site-id 2;
        }
      }
    }
  }
}

```

From configuration mode, confirm your configuration on Router PE2 by entering the **show protocols**, **show policy-options**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```

[edit]
user@PE2# show protocols
rsvp {
  interface all;
  interface fxp0.0 {
    disable;
  }
}

```

```
}
mpls {
  interface all;
  interface fxp0.0 {
    disable;
  }
  egress-protection {
    context-identifier 203.0.113.1 {
      protector;
      advertise-mode stub-alias;
    }
    traceoptions {
      file ep size 100m;
      flag all;
    }
  }
}
}
bgp {
  traceoptions {
    file bgp.log world-readable;
  }
  group ibgp {
    type internal;
    local-address 10.255.183.57;
    family inet {
      unicast;
    }
    family l2vpn {
      signaling {
        egress-protection;
      }
    }
    neighbor 192.0.2.3;
    neighbor 192.0.2.4;
  }
}
isis {
  traceoptions {
    file isis-edge size 10m world-readable;
    flag error;
  }
  level 1 disable;
  level 2 wide-metrics-only;
  interface all {
    point-to-point;
    level 2 metric 10;
  }
  interface fxp0.0 {
    disable;
  }
}
ldp {
  interface all;
  interface fxp0.0 {
    disable;
  }
}
```

```

}

[edit]
user@PE2# show policy-options
policy-statement lb {
    then {
        load-balance per-packet;
    }
}

[edit]
user@PE2# show routing-options
traceoptions {
    file ro.log;
    flag normal;
    flag route;
}
autonomous-system 100;
forwarding-table {
    export lb;
}

[edit]
user@PE2# show routing-instances
foo {
    instance-type l2vpn;
    egress-protection {
        protector;
    }
    interface ge-2/0/2.0;
    route-distinguisher 10.255.183.57:1;
    vrf-target target:9000:1;
    protocols {
        l2vpn {
            encapsulation-type ethernet-vlan;
            site foo {
                hot-standby;
                site-identifier 1;
                multi-homing;
                site-preference backup;
                interface ge-2/0/2.0 {
                    remote-site-id 2;
                }
            }
        }
    }
}
}

```

From configuration mode, confirm your configuration on Router PE3 by entering the **show protocols**, **show policy-options**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```

[edit]
user@PE3# show protocols

```

```
rsvp {
  interface all;
  interface fxp0.0 {
    disable;
  }
}
mpls {
  interface all;
  interface fxp0.0 {
    disable;
  }
}
bgp {
  traceoptions {
    file bgp.log world-readable;
  }
  group ibgp {
    type internal;
    local-address 10.255.183.61;
    family inet {
      unicast;
    }
    family l2vpn {
      signaling;
    }
    neighbor 192.0.2.3;
    neighbor 192.0.2.4;
  }
}
isis {
  traceoptions {
    file isis-edge size 10m world-readable;
    flag error;
  }
  level 1 disable;
  level 2 wide-metrics-only;
  interface all {
    point-to-point;
    level 2 metric 10;
  }
  interface fxp0.0 {
    disable;
  }
}
ldp {
  interface all;
  interface fxp0.0 {
    disable;
  }
}

[edit]
user@PE3# show policy-options
policy-statement lb {
  then {
```



```

        load-balance per-packet;
    }
}

[edit]
user@PE3# show routing-options
traceoptions {
    file ro.log;
    flag normal;
    flag route;
}
autonomous-system 100;
forwarding-table {
    export lb;
}

[edit]
user@PE3# show routing-instances
foo {
    instance-type l2vpn;
    interface ge-2/1/2.0;
    route-distinguisher 10.255.183.61:1;
    vrf-target target:9000:1;
    protocols {
        l2vpn {
            encapsulation-type ethernet-vlan;
            site foo {
                site-identifier 2;
                interface ge-2/1/2.0 {
                    remote-site-id 1;
                }
            }
        }
    }
}
}

```

Verification

Confirm that the configuration is working properly.

- [Verifying the L2VPN Configuration on page 485](#)
- [Verifying the Routing Instance Details on page 486](#)
- [Verifying the IS-IS Configuration on page 487](#)
- [Verifying the MPLS Configuration on page 487](#)

Verifying the L2VPN Configuration

Purpose Verify that LSP is protected by the connection protection logic.

Action From operational mode, run the **show l2vpn connections extensive** command.

```
user@PE2> show l2vpn connections extensive
```

```
Layer-2 VPN connections:
Legend for connection status (St)
EI -- encapsulation invalid      NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch     WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down   NP -- interface hardware not present
CM -- control-word mismatch     -> -- only outbound connection is up
CN -- circuit not provisioned   <- -- only inbound connection is up
OR -- out of range             Up -- operational
OL -- no outgoing label        Dn -- down
LD -- local site signaled down  CF -- call admission control failure
RD -- remote site signaled down SC -- local and remote site ID collision
LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status IL -- no incoming label
MM -- MTU mismatch             MI -- Mesh-Group ID not available
BK -- Backup connection        ST -- Standby connection
PF -- Profile parse failure     PB -- Profile busy
RS -- remote site standby       SN -- Static Neighbor
LB -- Local site not best-site  RB -- Remote site not best-site
VM -- VLAN ID mismatch

Legend for interface status
Up -- operational
Dn -- down
Instance: foo
Local site: foo (1)
  connection-site      Type  St  Time last up      # Up trans
    2                  rmt  Up  Aug 3 00:08:14 2001      1
    Local circuit: ge-2/0/2.0, Status: Up
    Remote PE: 192.0.2.3
    Incoming label: 32769, Outgoing label: 32768
    Egress Protection: Yes
      Time      Event      Interface/Lbl/PE
      Aug 3 00:08:14 2001 PE route up
      Aug 3 00:08:14 2001 Out lbl Update      32768
      Aug 3 00:08:14 2001 In lbl Update      32769
      Aug 3 00:08:14 2001 ckt0 up      fe-0/0/0.0
```

Meaning The **Egress Protection: Yes** output shows that the given PVC is protected by connection protection logic.

Verifying the Routing Instance Details

Purpose Verify the routing instance information and the context identifier configured on the primary, which is used as the next-hop address in case of node-link failure.

Action From operational mode, run the **show route foo detail** command.

```
user@PE2> show route foo detail
```

```
foo:
  Router ID: 0.0.0.0
  Type: l2vpn non-forwarding State: Active
  Interfaces:
    lt-1/2/0.56
  Route-distinguisher: 10.255.255.11:1
  Vrf-import: [ __vrf-import-foo-internal__ ]
```

```

Vrf-export: [ __vrf-export-foo-internal__ ]
Vrf-import-target: [ target:100:200 ]
Vrf-export-target: [ target:100:200 ]
Fast-reroute-priority: low
Vrf-edge-protection-id: 203.0.113.1
Tables:
  foo.l2vpn.0          : 5 routes (3 active, 0 holddown, 0 hidden)
  foo.l2id.0           : 6 routes (2 active, 0 holddown, 0 hidden)

```

Meaning The context-id is set to 203.0.113.1 and the Vrf-import: [__vrf-import-foo-internal__] in the output mentions the policy used for rewriting the next-hop address.

Verifying the IS-IS Configuration

Purpose Verify the IS-IS context identifier information.

Action From operational mode, run the **show isis context-identifier detail** command.

```

user@PE2> show isis context-identifier detail

IS-IS context database:
Context      L  Owner      Role      Primary      Metric
203.0.113.1  2  MPLS      Protector  pro17-b-lr-R1 0
  Advertiser pro17-b, Router ID 10.255.107.49, Level 2, tlv protector
  Advertiser pro17-b-lr-R1, Router ID 10.255.255.11, Metric 1, Level 2, tlv prefix

```

Meaning Router PE2 is the protector and the configured context identifier is in use for the MPLS protocol.

Verifying the MPLS Configuration

Purpose Verify the context identifier details on the primary and protector PEs.

Action From operational mode, run the **show mpls context-identifier detail** command.

```

user@PE1> show mpls context-identifier detail

ID: 203.0.113.1
  Type: primary, Metric: 1, Mode: alias

Total 1, Primary 1, Protector 0

user@PE2> show mpls context-identifier detail

ID: 203.0.113.1
  Type: protector, Metric: 16777215, Mode: alias
  Context table: __203.0.113.1__.mpls.0, Label out: 299968

user@PE2> show mpls egress-protection detail

Instance      Type      Protection-Type
foo            local-l2vpn  Protector
  Route Target 100:200

```

Meaning Context-id is **203.0.113.1**, advertise-mode is **alias**, the MPLS table created for egress protection is **__203.0.113.1__mpls.0**, and the egress instance name is **foo**, which is of type **local-l2vpn**.

Related Documentation

- [\[edit routing-instances\] Hierarchy Level](#)
- [site-preference on page 1196](#)

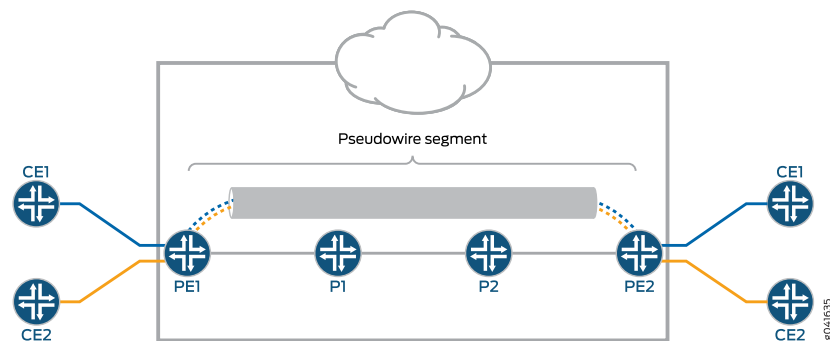
Understanding Multisegment Pseudowire for FEC 129

Understanding Multisegment Pseudowire

A pseudowire is a Layer 2 circuit or service that emulates the essential attributes of a telecommunications service, such as a T1 line, over an MPLS packet-switched network (PSN). The pseudowire is intended to provide only the minimum necessary functionality to emulate the wire with the required resiliency requirements for the given service definition.

When a pseudowire originates and terminates on the edge of the same PSN, the pseudowire label is unchanged between the originating and terminating provider edge (T-PE) devices. This is called a single-segment pseudowire (SS-PW). [Figure 40 on page 451](#) illustrates an SS-PW established between two PE routers. The pseudowires between the PE1 and PE2 routers are located within the same autonomous system (AS).

Figure 44: L2VPN Pseudowire

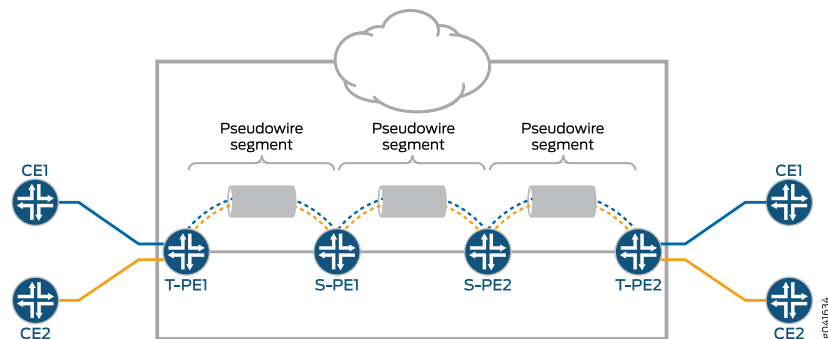


In cases where it is impossible to establish a single pseudowire from a local to a remote PE, either because it is unfeasible or undesirable to establish a single control plane between the two PEs, a multisegment pseudowire (MS-PW) is used.

An MS-PW is a set of two or more contiguous SS-PWs that are made to function as a single point-to-point pseudowire. It is also known as switched pseudowire. MS-PWs can go across different regions or network domains. A region can be considered as an interior gateway protocol (IGP) area or a BGP autonomous system that belongs to the same or different administrative domain. An MS-PW spans multiple cores or ASs of the same or different carrier networks. A Layer 2 VPN MS-PW can include up to 254 pseudowire segments.

Figure 41 on page 452 illustrates a set of two or more pseudowire segments that function as a single pseudowire. The end routers are called terminating PE (T-PE) routers, and the switching routers are called switching PE (S-PE) routers. The S-PE router terminates the tunnels of the preceding and succeeding pseudowire segments in an MS-PW. The S-PE router can switch the control and data planes of the preceding and succeeding pseudowire segments of the MS-PW. An MS-PW is declared to be up when all the single-segment pseudowires are up.

Figure 45: Multisegment Pseudowire



Using FEC 129 for Multisegment Pseudowire

Currently, there are two types of attachment circuit identifiers (AII) defined under FEC 129:

- Type 1 AII
- Type 2 AII

The support of an MS-PW for FEC 129 uses type 2 AII. A type 2 AII is globally unique by definition of RFC 5003.

Single-segment pseudowires (SS-PWs) using FEC 129 on an MPLS PSN can use both type 1 and type 2 AII. For an MS-PW using FEC 129, a pseudowire itself is identified as a pair of endpoints. This requires that the pseudowire endpoints be uniquely identified.

In the case of a dynamically placed MS-PW, there is a requirement for the identifiers of attachment circuits to be globally unique, for the purposes of reachability and manageability of the pseudowire. Thus, individual globally unique addresses are allocated to all the attachment circuits and S-PEs that make up an MS-PW.

Type 2 AII is composed of three fields:

- Global_ID—Global identification, which is usually the AS number.
- Prefix—IPv4 address, which is usually the router ID.
- AC_ID—Local attachment circuit, which is a user-configurable value.

Since type 2 All already contains the T-PE's IP address and it is globally unique, from the FEC 129 pseudowire signaling point of view, the combination (AGI, SAll, TAll) uniquely identifies an MS-PW across all interconnected pseudowire domains.

Establishing a Multisegment Pseudowire Overview

An MS-PW is established by dynamically and automatically selecting the predefined S-PEs and placing the MS-PW between two T-PE devices.

When S-PEs are dynamically selected, each S-PE is automatically discovered and selected using the BGP autodiscovery feature, without the requirement of provisioning the FEC 129 pseudowire-related information on all the S-PEs. BGP is used to propagate pseudowire address information throughout the PSN.

Since there is no manual provisioning of FEC 129 pseudowire information on the S-PEs, the Attachment Group Identifier (AGI) and Attachment Individual Identifier (All) are reused automatically, and choosing the same set of S-PEs for the pseudowire in both the forwarding and reverse direction is achieved through the active and passive role of each T-PE device.

- Active—The T-PE initiates an LDP label mapping message.
- Passive—The T-PE does not initiate an LDP label mapping message until it receives a label mapping message initiated by the active T-PE. The passive T-PE sends its label mapping message to the same S-PE from where it received the label mapping message originated from its active T-PE. This ensures that the same set of S-PEs are used in the reverse direction.

Pseudowire Status Support for Multisegment Pseudowire

- [Pseudowire Status Behavior on T-PE on page 490](#)
- [Pseudowire Status Behavior on S-PE on page 490](#)

Pseudowire Status Behavior on T-PE

The following pseudowire status messages are relevant on the T-PE:

- 0x00000010—Local PSN-facing pseudowire (egress) transmit fault.
- 0x00000001—Generic nonforwarding fault code. This is set as the local fault code. The local fault code is set at the local T-PE, and LDP sends a pseudowire status TLV message with the same fault code to the remote T-PE.
- Fault codes are bit-wise OR'ed and stored as remote pseudowire status codes.

Pseudowire Status Behavior on S-PE

The S-PE initiates the pseudowire status messages that indicate the pseudowire faults. The SP-PE in the pseudowire notification message hints where the fault was originated.

- When a local fault is detected by the S-PE, a pseudowire status message is sent in both directions along the pseudowire. Since there are no attachment circuits on an S-PE, only the following status messages are relevant:

- 0x00000008—Local PSN-facing pseudowire (ingress) receive fault.
- 0x00000010—Local PSN-facing pseudowire (egress) transmit fault.
- To indicate which SS-PW is at fault, an LDP SP-PE TLV is attached with the pseudowire status code in the LDP notification message. The pseudowire status is passed along from one pseudowire to another unchanged by the control plane switching function.
- If an S-PE initiates a pseudowire status notification message with one particular pseudowire status bit, then for the pseudowire status code an S-PE receives, the same bit is processed locally and not forwarded until the S-PE's original status error is cleared.
- An S-PE keeps only two pseudowire status codes for each SS-PW it is involved in – local pseudowire status code and remote pseudowire status code. The value of the remote pseudowire status code is the result of logic or operation of the pseudowire status codes in the chain of SS-PWs preceding this segment. This status code is incrementally updated by each S-PE upon receipt and communicated to the next S-PE. The local pseudowire status is generated locally based on its local pseudowire status.
- Only transmit fault is detected at the SP-PE. When there is no MPLS LSP to reach the next segment, a local transmit fault is detected. The transmit fault is sent to the next downstream segment, and the receive fault is sent to the upstream segment.
- Remote failures received on an S-PE are just passed along the MS-PW unchanged. Local failures are sent to both segments of the pseudowire that the S-PE is involved in.

Pseudowire TLV Support for MS-PW

MS-PW provides the following support for the LDP SP-PE TLV [RFC 6073]:

- The LDP SP-PE TLVs for an MS-PW include:
 - Local IP address
 - Remote IP address
- An SP-PE adds the LDP SP-PE TLV to the label mapping message. Each SP-PE appends the local LDP SP-PE TLV to the SP-PE list it received from the other segment.
- The pseudowire status notification message includes the LDP SP-PE TLV when the notification is generated at the SP-PE.

Supported and Unsupported Features

Junos OS supports the following features with MS-PW:

- MPLS PSN for each SS-PW that builds up the MS-PW.
- The same pseudowire encapsulation for each SS-PW in an MS-PW – Ethernet or VLAN-CCC.
- The generalized PWid FEC with T-LDP as an end-to-end pseudowire signaling protocol to set up each SS-PW.

- MP-BGP to autodiscover the two endpoint PEs for each SS-PW associated with the MS-PW.
- Standard MPLS operation to stitch two side-by-side SS-PWs to form an MS-PW.
- Automatic discovery of S-PE so that the MS-PW can be dynamically placed.
- Minimum provisioning of S-PE.
- Operation, administration, and maintenance (OAM) mechanisms, including end-to-end MPLS ping or end-to-any-S-PE MPLS ping, MPLS path trace, end-to-end VCCV, and Bidirectional Forwarding Detection (BFD).
- Pseudowire swithing point (SP) PE TLV for the MS-PW.
- Composite next hop on MS-PW.
- Pseudowire status TLV for MS-PW.

Junos OS does not support the following MS-PW functionality:

- Mix of LDP FEC 128 and LDP FEC 129.
- Static pseudowire where each label is provisioned statically.
- Graceful Routing Engine switchover.
- Nonstop active routing.
- Multihoming.
- Partial connectivity verification (originating from an S-PE) in OAM.

**Related
Documentation**

- [Example: Configuring a Multisegment Pseudowire on page 492](#)
- [Example: Configuring FEC 129 BGP Autodiscovery for VPWS on page 708](#)

Example: Configuring a Multisegment Pseudowire

This example shows how to configure a dynamic multisegment pseudowire (MS-PW), where the stitching provider edge (S-PE) devices are automatically and dynamically discovered by BGP, and pseudowires are signaled by LDP using FEC 129. This arrangement requires minimum provisioning on the S-PEs, thereby reducing the configuration burden that is associated with statically configured Layer 2 circuits while still using LDP as the underlying signaling protocol.

- [Requirements on page 493](#)
- [Overview on page 493](#)
- [Configuration on page 498](#)
- [Verification on page 517](#)
- [Troubleshooting on page 532](#)

Requirements

This example uses the following hardware and software components:

- Six routers that can be a combination of M Series Multiservice Edge Routers, MX Series 3D Universal Edge Routers, T Series Core Routers, or PTX Series Packet Transport Routers.
 - Two remote PE devices configured as terminating PEs (T-PEs).
 - Two S-PEs configured as:
 - Route reflectors, in the case of interarea configuration.
 - AS boundary routers or route reflectors, in the case of inter-AS configuration.
- Junos OS Release 13.3 or later running on all the devices.

Before you begin:

1. Configure the device interfaces.
2. Configure OSPF or any other IGP protocol.
3. Configure BGP.
4. Configure LDP.
5. Configure MPLS.

Overview

Starting with Junos OS Release 13.3, you can configure an MS-PW using FEC 129 with LDP signaling and BGP autodiscovery in an MPLS packet-switched network (PSN). The MS-PW feature also provides operation, administration, and management (OAM) capabilities, such as ping, traceroute, and BFD, from the T-PE devices.

To enable autodiscovery of S-PEs in an MS-PW, include the **auto-discovery-mspw** statement at the **[edit protocols bgp group group-name family l2vpn]** hierarchy level.

```
family l2vpn {
  auto-discovery-mspw;
}
```

The automatic selection of S-PE and dynamic setting up of an MS-PW rely heavily on BGP. BGP network layer reachability information (NLRI) constructed for the FEC 129 pseudowire to autodiscover the S-PE is called an MS-PW NLRI [draft-ietf-pwe3-dynamic-ms-pw-15.txt]. The MS-PW NLRI is essentially a prefix consisting of a route distinguisher (RD) and FEC 129 source attachment identifier (SAII). It is referred to as a BGP autodiscovery (BGP-AD) route and is encoded as **RD:SAII**.

Only T-PEs that are provisioned with type 2 AIs initiate their own MS-PW NLRI respectively. Since a type 2 AI is globally unique, an MS-PW NLRI is used to identify a PE device to which the type 2 AI is provisioned. The difference between a type 1 AI and a type 2 AI requires that a new address family indicator (AFI) and subsequent address

family identifier (SAFI) be defined in BGP to support an MS-PW. The proposed AFI and SAFI value pair used to identify the MS-PW NLRI is 25 and 6, respectively (pending IANA allocation).

The AFI and SAFI values support autodiscovery of S-PEs and should be configured on both T-PEs that originate the routes, and the S-PEs that participate in the signaling.

Figure 46 on page 494 illustrates an inter-area MS-PW setup between two remote PE routers—T-PE1 and T-PE2. The Provider (P) routers are P1 and P2, and the S-PE routers are S-PE1 and S-PE2. The MS-PW is established between T-PE1 and T-PE2, and all the devices belong to the same AS—AS 100. Since S-PE1 and S-PE2 belong to the same AS, they act as route reflectors and are also known as RR 1 and RR 2, respectively.

Figure 47 on page 494 illustrates an inter-AS MS-PW setup. The MS-PW is established between T-PE1 and T-PE2, where T-PE1, P1, and S-PE1 belong to AS 1, and S-PE2, P2, and T-PE2 belong to AS 2. Since S-PE1 and S-PE2 belong to different ASs, they are configured as ASBR routers and are also known as ASBR 1 and ASBR 2, respectively.

Figure 46: Interarea Multisegment Pseudowire

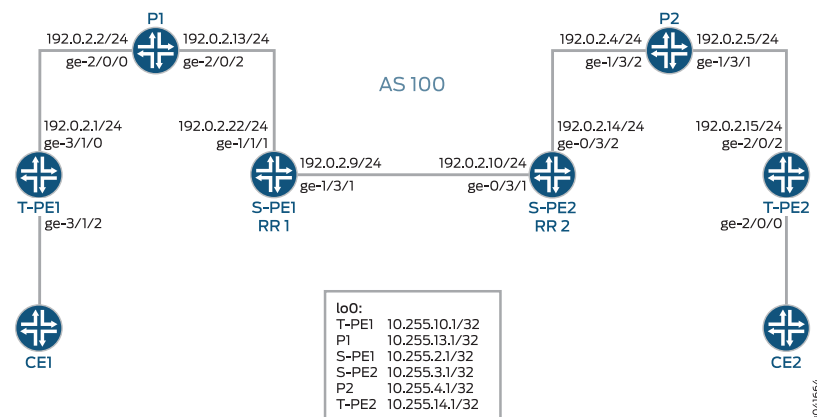
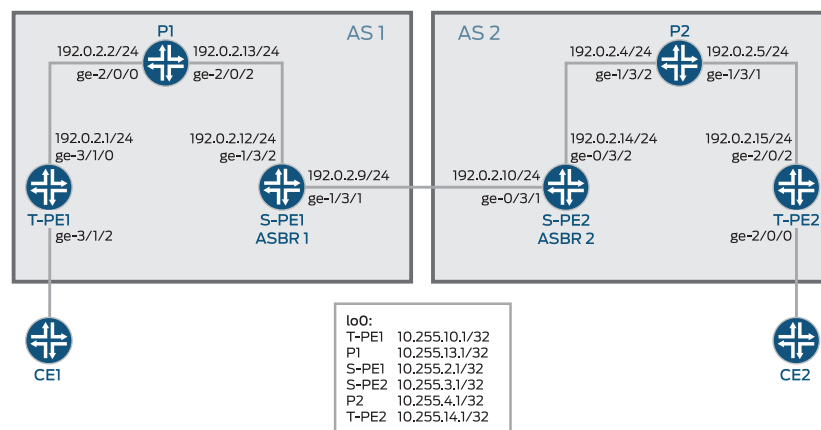


Figure 47: Inter-AS Multisegment Pseudowire



The following sections provide information about how an MS-PW is established in an interarea and inter-AS scenario.

Minimum Configuration Requirements on S-PE

In order to dynamically discover both ends of an SS-PW and set up a T-LDP session dynamically, the following is required:

- For interarea MS-PW, each S-PE plays both an ABR and BGP route reflector role.

In the interarea case, as seen in [Figure 46 on page 494](#), the S-PE plays a BGP route reflector role and reflects the BGP-AD route to its client. A BGP-AD route advertised by one T-PE eventually reaches its remote T-PE. Because of the next-hop-self set by each S-PE, the S-PE or T-PE that receives a BGP-AD route can always discover the S-PE that advertises the BGP-AD in its local AS or local area through the BGP next hop.

- For inter-AS MS-PW, each S-PE plays either an ASBR or a BGP route reflector role.

In an MS-PW, the two T-PEs initiate a BGP-AD route respectively. When the S-PE receives the BGP-AD route through either the IBGP session with the T-PE or through a regular BGP-RR, it sets the next-hop-self before re-advertising the BGP-AD route to one or more of its EBGP peers in the inter-AS case, as seen in [Figure 47 on page 494](#).

- Each S-PE must set next-hop-self when re-advertising or reflecting a BGP-AD route for the MS-PW.

Active and Passive Role of T-PE

To ensure that the same set of S-PEs are being used for a MS-PW in both directions, the two T-PEs play different roles in terms of FEC 129 signaling. This is to avoid different paths being chosen by T-PE1 and T-PE2 when each S-PE is dynamically selected for an MS-PW.

When an MS-PW is signaled using FEC 129, each T-PE might independently start signaling the MS-PW. The signaling procedure can result in an attempt to set up each direction of the MS-PW through different S-PEs.

To avoid this situation, one of the T-PEs must start the pseudowire signaling (active role), while the other waits to receive the LDP label mapping before sending the respective pseudowire LDP label mapping message (passive role). When the MS-PW path is dynamically placed, the active T-PE (the Source T-PE) and the passive T-PE (the Target T-PE) must be identified before signaling is initiated for a given MS-PW. The determination of which T-PE assumes the active role is done based on the SAll value, where the T-PE that has a larger SAll value plays the active role.

In this example, the SAll values of T-PE1 and T-PE 2 are **800:800:800** and **700:700:700**, respectively. Since T-PE1 has a higher SAll value, it assumes the active role and T-PE2 assumes the passive role.

Directions for Establishing an MS-PW

The directions used by the S-PE for setting up the MS-PW are:

- Forwarding direction—From an active T-PE to a passive T-PE.

In this direction, the S-PEs perform a BGP-AD route lookup to determine the next-hop S-PE to send the label mapping message.

- Reverse direction—From a passive T-PE to an active T-PE.

In this direction, the S-PEs do not perform a BGP-AD route lookup, because the label mapping messages are received from the T-PEs, and the stitching routes are installed in the S-PEs.

In this example, the MS-PW is established in the forwarding direction from T-PE1 to T-PE2. When the MS-PW is placed from T-PE2 to T-PE1, the MS-PW is established in the reverse direction.

Autodiscovery and Dynamic Selection of S-PE

A new AFI and SAFI value is defined in BGP to support the MS-PWs based on type 2 All. This new address family supports autodiscovery of S-PEs. This address family must be configured on both the T-PEs and S-PEs.

It is the responsibility of the Layer 2 VPN component to dynamically select the next S-PE to use along the MS-PW in the forwarding direction.

- In the forwarding direction, the selection of the next S-PE is based on the BGP-AD route advertised by the BGP and pseudowire FEC information sent by the LDP. The BGP-AD route is initiated by the passive T-PE (T-PE2) in the reverse direction while the pseudowire FEC information is sent by LDP from the active T-PE (T-PE1) in the forwarding direction.
- In the reverse direction, the next S-PE (S-PE2) or the active T-PE (T-PE1) is obtained by looking up the S-PE (S-PE1) that it used to set up the pseudowire in the forwarding direction.

Provisioning a T-PE

To support FEC 129 type 2 All, the T-PE needs to configure its remote T-PE's IP address, a global ID, and an attachment circuit ID. Explicit paths where a set of S-PEs to use is explicitly specified on a T-PE is not supported. This eliminates the need to provision each S-PE with a type 2 All.

Stitching an MS-PW

An S-PE performs the following MPLS label operations before forwarding the received label mapping message to the next S-PE:

1. Pops the MPLS tunnel label.
2. Pops the VC label.
3. Pushes a new VC label.
4. Pushes an MPLS tunnel label used for the next segment.

Establishing an MS-PW

After completing the necessary configuration, an MS-PW is established in the following manner:

1. The SAll values are exchanged between T-PE1 and T-PE2 using BGP.
T-PE1 assumes the active T-PE role, because it is configured with a higher SAll value. T-PE2 becomes the passive T-PE.
2. T-PE1 receives the BGP-AD route originated by T-PE2. It compares the All values obtained from T-PE2 in the received BGP-AD route against the All values provisioned locally.
3. If the All values match, T-PE1 performs a BGP-AD route lookup to elect the first S-PE (S-PE1).
4. T-PE1 sends an LDP label mapping message to S-PE1.
5. Using the BGP-AD route originated from T-PE2, and the LDP label mapping message received from T-PE1, S-PE1 selects the next S-PE (S-PE2) in the forwarding direction.
To do this, S-PE1 compares SAll obtained from the BGP-AD route against the TAI from the LDP label mapping message.
6. If the All values match, S-PE1 finds S-PE2 through the BGP next hop associated with the BGP-AD route.
7. The process of selecting S-PE goes on until the last S-PE establishes a T-LDP session with T-PE2. When T-PE2 receives the LDP label mapping message from the last S-PE (S-PE2), it initiates its own label mapping message and sends it back to S-PE2.
8. When all the label mapping messages are received on S-PE1 and S-PE2, the S-PEs install the stitching routes. Thus, when the MS-PW is established in the reverse direction, the S-PEs need not perform BGP-AD route lookup to determine its next hop as it did in the forwarding direction.

OAM Support for an MS-PW

After the MS-PW is established, the following OAM capabilities can be executed from the T-PE devices:

- Ping
 - End-to-End Connectivity Verification Between T-PEs

If T-PE1, S-PEs, and T-PE2 support Control Word (CW), the pseudowire control plane automatically negotiates the use of the CW. Virtual Circuit Connectivity Verification (VCCV) Control Channel (CC) Type 3 will function correctly whether or not the CW is enabled on the pseudowire. However, VCCV Type 1, which is used for end-to-end verification only, is only supported if the CW is enabled.

The following is a sample:

```
user@T-PE1> ping mpls l2vpn fec129 instance instance-name local-id SAll of T-PE1
remote-pe-address address of T-PE2 remote-id TAI of T-PE2
or
```

```
user@T-PE1> ping mpls l2vpn fec129 interface CE1-facing interface
```

- Partial Connectivity Verification from T-PE to Any S-PE

To trace part of an MS-PW, the TTL of the pseudowire label can be used to force the VCCV message to pop out at an intermediate node. When the TTL expires, the S-PE can determine that the packet is a VCCV packet either by checking the CW or by checking for a valid IP header with UDP destination port 3502 (if the CW is not in use). The packet should then be diverted to VCCV processing.

If T-PE1 sends a VCCV message with the TTL of the pseudowire label equal to 1, the TTL expires at the S-PE. T-PE1 can thus verify the first segment of the pseudowire.

The VCCV packet is built according to RFC 4379. All the information necessary to build the VCCV LSP ping packet is collected by inspecting the S-PE TLVs. This use of the TTL is subject to the caution expressed in RFC 5085. If a penultimate LSR between S-PEs or between an S-PE and a T-PE manipulates the pseudowire label TTL, the VCCV message might not emerge from the MS-PW at the correct S-PE.

The following is a sample:

```
user@T-PE1> ping mpls l2vpn fec129 interface CE1-facing interface bottom-label-ttl segment
```

The **bottom-label-ttl** value is 1 for S-PE1 and 2 for S-PE2.

The **bottom-label-ttl** statement sets the correct VC label TTL, so the packets are popped to the correct SS-PW for VCCV processing.



NOTE: Junos OS supports VCCV Type 1 and Type 3 for the MS-PW OAM capability. VCCV Type 2 is not supported.

- Traceroute

Traceroute tests each S-PE along the path of the MS-PW in a single operation similar to LSP trace. This operation is able to determine the actual data path of the MS-PW, and is used for dynamically signaled MS-PWs.

```
user@T-PE1> traceroute mpls l2vpn fec129 interface CE1-facing interface
```

- Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. The router or switch can be configured to log a system log (syslog) message when BFD goes down.

```
user@T-PE1> show bfd session extensive
```

Configuration

- [Configuring an Interarea MS-PW on page 499](#)
- [Configuring an Inter-AS MS-PW on page 508](#)

Configuring an Interarea MS-PW

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.
T-PE1	<pre> set interfaces ge-3/1/0 unit 0 family inet address 192.0.2.1/24 set interfaces ge-3/1/0 unit 0 family mpls set interfaces ge-3/1/2 encapsulation ethernet-ccc set interfaces ge-3/1/2 unit 0 set interfaces lo0 unit 0 family inet address 10.255.10.1/32 primary set routing-options autonomous-system 100 set protocols mpls interface all set protocols mpls interface fxp0.0 disable set protocols bgp family l2vpn auto-discovery-mspw set protocols bgp group mspw type internal set protocols bgp group mspw local-address 10.255.10.1 set protocols bgp group mspw neighbor 10.255.2.1 set protocols ospf area 0.0.0.0 interface lo0.0 set protocols ospf area 0.0.0.0 interface all set protocols ospf area 0.0.0.0 interface fxp0.0 disable set protocols ldp interface all set protocols ldp interface fxp0.0 disable set protocols ldp interface lo0.0 set routing-instances ms-pw instance-type l2vpn set routing-instances ms-pw interface ge-3/1/2.0 set routing-instances ms-pw route-distinguisher 10.10.10.15 set routing-instances ms-pw l2vpn-id l2vpn-id:100:15 set routing-instances ms-pw vrf-target target:100:115 set routing-instances ms-pw protocols l2vpn site CE1 source-attachment-identifier 800:800:800 set routing-instances ms-pw protocols l2vpn site CE1 interface ge-3/1/2.0 target-attachment-identifier 700:700:700 set routing-instances ms-pw protocols l2vpn pseudowire-status-tlv set routing-instances ms-pw protocols l2vpn oam bfd-liveness-detection minimum-interval 300 </pre>
P1	<pre> set interfaces ge-2/0/0 unit 0 family inet address 192.0.2.2/24 set interfaces ge-2/0/0 unit 0 family mpls set interfaces ge-2/0/2 unit 0 family inet address 192.0.2.13/24 set interfaces ge-2/0/2 unit 0 family mpls set interfaces lo0 unit 0 family inet address 10.255.13.1/32 primary set routing-options autonomous-system 100 set protocols mpls interface all set protocols mpls interface fxp0.0 disable set protocols ospf area 0.0.0.0 interface lo0.0 set protocols ospf area 0.0.0.0 interface all set protocols ospf area 0.0.0.0 interface fxp0.0 disable set protocols ldp interface all set protocols ldp interface fxp0.0 disable set protocols ldp interface lo0.0 </pre>
S-PE1 (RR 1)	<pre> set interfaces ge-1/3/1 unit 0 family inet address 192.0.2.9/24 set interfaces ge-1/3/1 unit 0 family mpls </pre>

```

set interfaces ge-1/3/2 unit 0 family inet address 192.0.2.12/24
set interfaces ge-1/3/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.2.1/32 primary
set routing-options autonomous-system 100
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols bgp family l2vpn auto-discovery-mspw
set protocols bgp group mspw type internal
set protocols bgp group mspw local-address 10.255.2.1
set protocols bgp group mspw export next-hop-self
set protocols bgp group mspw cluster 198.51.100.1
set protocols bgp group mspw neighbor 10.255.10.1
set protocols bgp group mspw neighbor 10.255.3.1
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0
set policy-options policy-statement next-hop-self then next-hop self
set policy-options policy-statement send-inet0 from protocol bgp
set policy-options policy-statement send-inet0 then accept

```

S-PE2 (RR 2)

```

set interfaces ge-0/3/1 unit 0 family inet address 192.0.2.10/24
set interfaces ge-0/3/1 unit 0 family mpls
set interfaces ge-0/3/2 unit 0 family inet address 192.0.2.14/24
set interfaces ge-0/3/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.3.1/32 primary
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols bgp family l2vpn auto-discovery-mspw
set protocols bgp group mspw type internal
set protocols bgp group mspw local-address 10.255.3.1
set protocols bgp group mspw export next-hop-self
set protocols bgp group mspw cluster 198.51.100.2
set protocols bgp group mspw neighbor 10.255.2.1
set protocols bgp group mspw neighbor 10.255.14.1
set protocols bgp group int type internal
set protocols bgp group int local-address 10.255.3.1
set protocols bgp group int neighbor 10.255.2.1
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0
set policy-options policy-statement next-hop-self then next-hop self
set policy-options policy-statement send-inet0 from protocol bgp
set policy-options policy-statement send-inet0 then accept

```

P2

```

set interfaces ge-1/3/1 unit 0 family inet address 192.0.2.5/24
set interfaces ge-1/3/1 unit 0 family mpls
set interfaces ge-1/3/2 unit 0 family inet address 192.0.2.4/24
set interfaces ge-1/3/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.4.1/32 primary

```



```

set routing-options autonomous-system 100
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0

```

```

T-PE2 set interfaces ge-2/0/0 encapsulation ethernet-ccc
set interfaces ge-2/0/0 unit 0
set interfaces ge-2/0/2 unit 0 family inet address 192.0.2.15/24
set interfaces ge-2/0/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.14.1/32 primary
set routing-options autonomous-system 100
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols bgp family l2vpn auto-discovery-mspw
set protocols bgp group mspw type internal
set protocols bgp group mspw local-address 10.255.14.1
set protocols bgp group mspw neighbor 10.255.3.1
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0
set routing-instances ms-pw instance-type l2vpn
set routing-instances ms-pw interface ge-2/0/0.0
set routing-instances ms-pw route-distinguisher 10.10.10.15
set routing-instances ms-pw l2vpn-id l2vpn-id:100:15
set routing-instances ms-pw vrf-target target:100:15
set routing-instances ms-pw protocols l2vpn site CE2 source-attachment-identifier
700:700:700
set routing-instances ms-pw protocols l2vpn site CE2 interface ge-2/0/0.0
target-attachment-identifier 800:800:800
set routing-instances ms-pw protocols l2vpn pseudowire-status-tlv
set routing-instances ms-pw protocols l2vpn oam bfd-liveness-detection
minimum-interval 300

```

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 T-PE1 in the interarea scenario:



NOTE: Repeat this procedure for the T-PE2 device in the MPLS domain, after modifying the appropriate interface names, addresses, and other parameters.

1. Configure the T-PE1 interfaces.

[edit interfaces]

```
user@T-PE1# set ge-3/1/0 unit 0 family inet address 192.0.2.1/24
```

```
user@T-PE1# set ge-3/1/0 unit 0 family mpls
```

```
user@T-PE1# set ge-3/1/2 encapsulation ethernet-ccc
```

```
user@T-PE1# set ge-3/1/2 unit 0
```

```
user@T-PE1# set lo0 unit 0 family inet address 10.255.10.1/32 primary
```

2. Set the autonomous system number.

[edit routing-options]

```
user@T-PE1# set autonomous-system 100
```

3. Enable MPLS on all the interfaces of T-PE1, excluding the management interface.

[edit protocols]

```
user@T-PE1# set mpls interface all
```

```
user@T-PE1# set mpls interface fxp0.0 disable
```

4. Enable autodiscovery of intermediate S-PEs that make up the MS-PW using BGP.

[edit protocols]

```
user@T-PE1# set bgp family l2vpn auto-discovery-mspw
```

5. Configure the BGP group for T-PE1.

[edit protocols]

```
user@T-PE1# set bgp group mspw type internal
```

6. Assign local and neighbor addresses to the mspw group for T-PE1 to peer with S-PE1.

[edit protocols]

```
user@T-PE1# set bgp group mspw local-address 10.255.10.1
```

```
user@T-PE1# set bgp group mspw neighbor 10.255.2.1
```

7. Configure OSPF on all the interfaces of T-PE1, excluding the management interface.

[edit protocols]

```
user@T-PE1# set ospf area 0.0.0.0 interface lo0.0
```

```
user@T-PE1# set ospf area 0.0.0.0 interface all
```

```
user@T-PE1# set ospf area 0.0.0.0 interface fxp0.0 disable
```

8. Configure LDP on all the interfaces of T-PE1, excluding the management interface.

[edit protocols]

```
user@T-PE1# set ldp interface all
```

```
user@T-PE1# set ldp interface fxp0.0 disable
```

```
user@T-PE1# set ldp interface lo0.0
```

9. Configure the Layer 2 VPN routing instance on T-PE1.

[edit routing-instances]

```
user@T-PE1# set ms-pw instance-type l2vpn
```

10. Assign the interface name for the mspw routing instance.

[edit routing-instances]

```
user@T-PE1# set ms-pw interface ge-3/1/2.0
```

11. Configure the route distinguisher for the mspw routing instance.

```
[edit routing-instances]
user@T-PE1# set ms-pw route-distinguisher 10.10.10.10:15
```

12. Configure the Layer 2 VPN ID community for FEC 129 MS-PW.

```
[edit routing-instances]
user@T-PE1# set ms-pw l2vpn-id l2vpn-id:100:15
```

13. Configure a VPN routing and forwarding (VRF) target for the mspw routing instance.

```
[edit routing-instances]
user@T-PE1# set ms-pw vrf-target target:100:115
```

14. Configure the source attachment identifier (SAI) value using Layer 2 VPN as the routing protocol for the mspw routing instance.

```
[edit routing-instances]
user@T-PE1# set ms-pw protocols l2vpn site CE1 source-attachment-identifier
800:800:800
```

15. Assign the interface name that connects the CE1 site to the VPN, and configure the target attachment identifier (TAI) value using Layer 2 VPN as the routing protocol for the mspw routing instance.

```
[edit routing-instances]
user@T-PE1# set ms-pw protocols l2vpn site CE1 interface ge-3/1/2.0
target-attachment-identifier 700:700:700
```

16. (Optional) Configure T-PE1 to send MS-PW status TLVs.

```
[edit routing-instances]
user@T-PE1# set ms-pw protocols l2vpn pseudowire-status-tlv
```

17. (Optional) Configure OAM capabilities for the VPN.

```
[edit routing-instances]
user@T-PE1# set ms-pw protocols l2vpn oam bfd-liveness-detection
minimum-interval 300
```

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 S-PE1 (RR 1) in the interarea scenario:



NOTE: Repeat this procedure for the S-PE2 (RR 2) device in the MPLS domain, after modifying the appropriate interface names, addresses, and other parameters.

1. Configure the S-PE1 interfaces.

```
[edit interfaces]
user@S-PE1# set ge-1/3/1 unit 0 family inet address 192.0.2.9/24
user@S-PE1# set ge-1/3/1 unit 0 family mpls
```

```
user@S-PE1# set ge-1/3/2 unit 0 family inet address 192.0.2.12/24
```

```
user@S-PE1# set ge-1/3/2 unit 0 family mpls
```

```
user@S-PE1# set lo0 unit 0 family inet address 10.255.2.1/32 primary
```

2. Set the autonomous system number.

```
[edit routing-options]
```

```
user@S-PE1# set autonomous-system 100
```

3. Enable MPLS on all the interfaces of T-PE1, excluding the management interface.

```
[edit protocols]
```

```
user@S-PE1# set mpls interface all
```

```
user@S-PE1# set mpls interface fxp0.0 disable
```

4. Enable autodiscovery of S-PE using BGP.

```
[edit protocols]
```

```
user@S-PE1# set bgp family l2vpn auto-discovery-mspw
```

5. Configure the BGP group for S-PE1.

```
[edit protocols]
```

```
user@S-PE1# set bgp group mspw type internal
```

6. Configure S-PE1 to act as a route reflector.

```
[edit protocols]
```

```
user@S-PE1# set bgp group mspw export next-hop-self
```

```
user@S-PE1# set bgp group mspw cluster 198.51.100.1
```

7. Assign local and neighbor addresses to the mspw group for S-PE1 to peer with T-PE1 and S-PE2.

```
[edit protocols]
```

```
user@S-PE1# set bgp group mspw local-address 10.255.2.1
```

```
user@S-PE1# set bgp group mspw neighbor 10.255.10.1 (to T-PE1)
```

```
user@S-PE1# set bgp group mspw neighbor 10.255.3.1 (to S-PE2)
```

8. Configure OSPF on all the interfaces of S-PE1, excluding the management interface.

```
[edit protocols]
```

```
user@S-PE1# set ospf area 0.0.0.0 interface all
```

```
user@S-PE1# set ospf area 0.0.0.0 interface fxp0.0 disable
```

```
user@S-PE1# set ospf area 0.0.0.0 interface lo0.0
```

9. Configure LDP on all the interfaces of S-PE1, excluding the management interface.

```
[edit protocols]
```

```
user@S-PE1# set ldp interface all
```

```
user@S-PE1# set ldp interface fxp0.0 disable
```

```
user@S-PE1# set ldp interface lo0.0
```

10. Define the policy for enabling next-hop-self and accepting BGP traffic on S-PE1.

```
[edit policy-options]
```

```
user@S-PE1# set policy-statement next-hop-self then next-hop self
```

```
user@S-PE1# set policy-statement send-inet0 from protocol bgp
```

```
user@S-PE1# set policy-statement send-inet0 then accept
```

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

```
T-PE1 user@T-PE1# show interfaces
ge-3/1/0 {
  unit 0 {
    family inet {
      address 192.0.2.1/24;
    }
    family mpls;
  }
}
ge-3/1/2 {
  encapsulation ethernet-ccc;
  unit 0;
}
lo0 {
  unit 0 {
    family inet {
      address 10.255.10.1/32 {
        primary;
      }
    }
  }
}

user@T-PE1# show routing-options
autonomous-system 100;

user@T-PE1# show protocols
mpls {
  interface all;
  interface fxp0.0 {
    disable;
  }
}
bgp {
  family l2vpn {
    auto-discovery-mspw;
  }
  group mspw {
    type internal;
    local-address 10.255.10.1;
    neighbor 10.255.2.1;
  }
}
ospf {
  area 0.0.0.0 {
    interface all;
    interface fxp0.0 {
      disable;
    }
    interface lo0.0;
  }
}
```

```

}
ldp {
  interface all;
  interface fxp0.0 {
    disable;
  }
  interface lo0.0;
}

user@T-PE1# show routing-instances
ms-pw {
  instance-type l2vpn;
  interface ge-3/1/2.0;
  route-distinguisher 10.10.10.10:15;
  l2vpn-id l2vpn-id:100:15;
  vrf-target target:100:115;
  protocols {
    l2vpn {
      site CE1 {
        source-attachment-identifier 800:800:800;
        interface ge-3/1/2.0 {
          target-attachment-identifier 700:700:700;
        }
      }
      pseudowire-status-tlv;
      oam {
        bfd-liveness-detection {
          minimum-interval 300;
        }
      }
    }
  }
}

S-PE1 (RR 1) user@S-PE1# show interfaces
ge-1/3/1 {
  unit 0 {
    family inet {
      address 192.0.2.9/24;
    }
    family mpls;
  }
}
ge-1/3/2 {
  unit 0 {
    family inet {
      address 192.0.2.12/24;
    }
    family mpls;
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.255.2.1/32 {
        primary;
      }
    }
  }
}

```

```

    }
  }
}

user@S-PE1# show routing-options
autonomous-system 100;

user@S-PE1# show protocols
mpls {
  interface all;
  interface fxp0.0 {
    disable;
  }
}
bgp {
  family l2vpn {
    auto-discovery-mspw;
  }
  group mspw {
    type internal;
    local-address 10.255.2.1;
    export next-hop-self;
    cluster 198.51.100.1;
    neighbor 10.255.10.1;
    neighbor 10.255.3.1;
  }
}
ospf {
  area 0.0.0.0 {
    interface lo0.0;
    interface all;
    interface fxp0.0 {
      disable;
    }
  }
}
ldp {
  interface all;
  interface fxp0.0 {
    disable;
  }
  interface lo0.0;
}

user@S-PE1# show policy-options
policy-statement next-hop-self {
  then {
    next-hop self;
  }
}
policy-statement send-inet0 {
  from protocol bgp;
  then accept;
}

```

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

Configuring an Inter-AS MS-PW

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.
T-PE1	<pre> set interfaces ge-3/1/0 unit 0 family inet address 192.0.2.1/24 set interfaces ge-3/1/0 unit 0 family mpls set interfaces ge-3/1/2 encapsulation ethernet-ccc set interfaces ge-3/1/2 unit 0 set interfaces lo0 unit 0 family inet address 10.255.10.1/32 primary set routing-options autonomous-system 1 set protocols mpls interface all set protocols mpls interface fxp0.0 disable set protocols bgp family l2vpn auto-discovery-mspw set protocols bgp group mspw type internal set protocols bgp group mspw local-address 10.255.10.1 set protocols bgp group mspw neighbor 10.255.2.1 set protocols ospf area 0.0.0.0 interface lo0.0 set protocols ospf area 0.0.0.0 interface all set protocols ospf area 0.0.0.0 interface fxp0.0 disable set protocols ldp interface all set protocols ldp interface fxp0.0 disable set protocols ldp interface lo0.0 set routing-instances ms-pw instance-type l2vpn set routing-instances ms-pw interface ge-3/1/2.0 set routing-instances ms-pw route-distinguisher 10.10.10.15 set routing-instances ms-pw l2vpn-id l2vpn-id:100:15 set routing-instances ms-pw vrf-target target:100:115 set routing-instances ms-pw protocols l2vpn site CE1 source-attachment-identifier 800:800:800 set routing-instances ms-pw protocols l2vpn site CE1 interface ge-3/1/2.0 target-attachment-identifier 700:700:700 set routing-instances ms-pw protocols l2vpn pseudowire-status-tlv set routing-instances ms-pw protocols l2vpn oam bfd-liveness-detection minimum-interval 300 </pre>
P1	<pre> set interfaces ge-2/0/0 unit 0 family inet address 192.0.2.2/24 set interfaces ge-2/0/0 unit 0 family mpls set interfaces ge-2/0/2 unit 0 family inet address 192.0.2.13/24 set interfaces ge-2/0/2 unit 0 family mpls set interfaces lo0 unit 0 family inet address 10.255.13.1/32 primary set routing-options autonomous-system 1 set protocols mpls interface all set protocols mpls interface fxp0.0 disable set protocols ospf area 0.0.0.0 interface lo0.0 set protocols ospf area 0.0.0.0 interface all set protocols ospf area 0.0.0.0 interface fxp0.0 disable set protocols ldp interface all set protocols ldp interface fxp0.0 disable set protocols ldp interface lo0.0 </pre>
S-PE1 (ASBR 1)	<pre> set interfaces ge-1/3/1 unit 0 family inet address 192.0.2.9/24 set interfaces ge-1/3/1 unit 0 family mpls </pre>


```

set interfaces ge-1/3/2 unit 0 family inet address 192.0.2.12/24
set interfaces ge-1/3/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.2.1/32 primary
set routing-options autonomous-system 1
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols bgp family l2vpn auto-discovery-mspw
set protocols bgp group to_T-PE1 type internal
set protocols bgp group to_T-PE1 local-address 10.255.2.1
set protocols bgp group to_T-PE1 export next-hop-self
set protocols bgp group to_T-PE1 neighbor 10.255.10.1
set protocols bgp group to_S-PE2 type external
set protocols bgp group to_S-PE2 local-address 10.255.2.1
set protocols bgp group to_S-PE2 peer-as 2
set protocols bgp group to_S-PE2 neighbor 10.255.3.1 multihop ttl 1
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0
set policy-options policy-statement next-hop-self then next-hop self

```

S-PE2 (ASBR 2)

```

set interfaces ge-0/3/1 unit 0 family inet address 192.0.2.10/24
set interfaces ge-0/3/1 unit 0 family mpls
set interfaces ge-0/3/2 unit 0 family inet address 192.0.2.14/24
set interfaces ge-0/3/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.3.1/32 primary
set routing-options autonomous-system 2
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols bgp family l2vpn auto-discovery-mspw
set protocols bgp group to_T-PE2 type internal
set protocols bgp group to_T-PE2 local-address 10.255.3.1
set protocols bgp group to_T-PE2 export next-hop-self
set protocols bgp group to_T-PE2 neighbor 10.255.14.1
set protocols bgp group to_S-PE1 type external
set protocols bgp group to_S-PE1 local-address 10.255.3.1
set protocols bgp group to_S-PE1 peer-as 1
set protocols bgp group to_S-PE1 neighbor 10.255.2.1 multihop ttl 1
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0
set policy-options policy-statement next-hop-self then next-hop self

```

P2

```

set interfaces ge-1/3/1 unit 0 family inet address 192.0.2.5/24
set interfaces ge-1/3/1 unit 0 family mpls
set interfaces ge-1/3/2 unit 0 family inet address 192.0.2.4/24
set interfaces ge-1/3/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.4.1/32 primary
set routing-options autonomous-system 2
set protocols mpls interface all

```

```

set protocols mpls interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0

```

```

T-PE2 set interfaces ge-2/0/0 encapsulation ethernet-ccc
set interfaces ge-2/0/0 unit 0
set interfaces ge-2/0/2 unit 0 family inet address 192.0.2.15/24
set interfaces ge-2/0/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.14.1/32 primary
set routing-options autonomous-system 2
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols bgp family l2vpn auto-discovery-mspw
set protocols bgp group mspw type internal
set protocols bgp group mspw local-address 10.255.14.1
set protocols bgp group mspw neighbor 10.255.3.1
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0
set routing-instances ms-pw instance-type l2vpn
set routing-instances ms-pw interface ge-2/0/0.0
set routing-instances ms-pw route-distinguisher 10.10.10.10:15
set routing-instances ms-pw l2vpn-id l2vpn-id:100:15
set routing-instances ms-pw vrf-target target:100:115
set routing-instances ms-pw protocols l2vpn site CE2 source-attachment-identifier
700:700:700
set routing-instances ms-pw protocols l2vpn site CE2 interface ge-2/0/0.0
target-attachment-identifier 800:800:800
set routing-instances ms-pw protocols l2vpn pseudowire-status-tlv
set routing-instances ms-pw protocols l2vpn oam bfd-liveness-detection
minimum-interval 300

```

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 T-PE1 router in the inter-AS scenario:



NOTE: Repeat this procedure for the T-PE2 device in the MPLS domain, after modifying the appropriate interface names, addresses, and other parameters.

1. Configure the T-PE1 interfaces.

[edit interfaces]

```
user@T-PE1# set ge-3/1/0 unit 0 family inet address 192.0.2.1/24
```

```
user@T-PE1# set ge-3/1/0 unit 0 family mpls
```

```
user@T-PE1# set ge-3/1/2 encapsulation ethernet-ccc
user@T-PE1# set ge-3/1/2 unit 0
```

```
user@T-PE1# set lo0 unit 0 family inet address 10.255.10.1/32 primary
```

2. Set the autonomous system number.

```
[edit routing-options]
user@T-PE1# set autonomous-system 1
```

3. Enable MPLS on all the interfaces of T-PE1, excluding the management interface.

```
[edit protocols]
user@T-PE1# set mpls interface all
user@T-PE1# set mpls interface fxp0.0 disable
```

4. Enable autodiscovery of intermediate S-PEs that make up the MS-PW using BGP.

```
[edit protocols]
user@T-PE1# set bgp family l2vpn auto-discovery-mspw
```

5. Configure the BGP group for T-PE1.

```
[edit protocols]
user@T-PE1# set bgp group mspw type internal
```

6. Assign local and neighbor addresses to the mspw group for T-PE1 to peer with S-PE1.

```
[edit protocols]
user@T-PE1# set bgp group mspw local-address 10.255.10.1
user@T-PE1# set bgp group mspw neighbor 10.255.2.1
```

7. Configure OSPF on all the interfaces of T-PE1, excluding the management interface.

```
[edit protocols]
user@T-PE1# set ospf area 0.0.0.0 interface lo0.0
user@T-PE1# set ospf area 0.0.0.0 interface all
user@T-PE1# set ospf area 0.0.0.0 interface fxp0.0 disable
```

8. Configure LDP on all the interfaces of T-PE1, excluding the management interface.

```
[edit protocols]
user@T-PE1# set ldp interface all
user@T-PE1# set ldp interface fxp0.0 disable
user@T-PE1# set ldp interface lo0.0
```

9. Configure the Layer 2 VPN routing instance on T-PE1.

```
[edit routing-instances]
user@T-PE1# set ms-pw instance-type l2vpn
```

10. Assign the interface name for the mspw routing instance.

```
[edit routing-instances]
user@T-PE1# set ms-pw interface ge-3/1/2.0
```

11. Configure the route distinguisher for the mspw routing instance.

```
[edit routing-instances]
```

```
user@T-PE1# set ms-pw route-distinguisher 10.10.10.10:15
```

12. Configure the Layer 2 VPN ID community for FEC 129 MS-PW.

```
[edit routing-instances]
user@T-PE1# set ms-pw l2vpn-id l2vpn-id:100:15
```

13. Configure a VPN routing and forwarding (VRF) target for the mspw routing instance.

```
[edit routing-instances]
user@T-PE1# set ms-pw vrf-target target:100:115
```

14. Configure the source attachment identifier (SAI) value using Layer 2 VPN as the routing protocol for the mspw routing instance.

```
[edit routing-instances]
user@T-PE1# set ms-pw protocols l2vpn site CE1 source-attachment-identifier
800:800:800
```

15. Assign the interface name that connects the CE1 site to the VPN, and configure the target attachment identifier (TAI) value using Layer 2 VPN as the routing protocol for the mspw routing instance.

```
[edit routing-instances]
user@T-PE1# set ms-pw protocols l2vpn site CE1 interface ge-3/1/2.0
target-attachment-identifier 700:700:700
```

16. (Optional) Configure T-PE1 to send MS-PW status TLVs.

```
[edit routing-instances]
user@T-PE1# set ms-pw protocols l2vpn pseudowire-status-tlv
```

17. (Optional) Configure OAM capabilities for the VPN.

```
[edit routing-instances]
user@T-PE1# set ms-pw protocols l2vpn oam bfd-liveness-detection
minimum-interval 300
```

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 S-PE1 (ASBR 1) in the inter-AS scenario:



NOTE: Repeat this procedure for the S-PE2 (ASBR 2) device in the MPLS domain, after modifying the appropriate interface names, addresses, and other parameters.

1. Configure S-PE1 (ASBR 1) interfaces.

```
[edit interfaces]
user@S-PE1# set ge-1/3/1 unit 0 family inet address 192.0.2.9/24
user@S-PE1# set ge-1/3/1 unit 0 family mpls
```

```
user@S-PE1# set ge-1/3/2 unit 0 family inet address 192.0.2.12/24
user@S-PE1# set ge-1/3/2 unit 0 family mpls
```

- ```

user@S-PE1# set lo0 unit 0 family inet address 10.255.2.1/32 primary

```
2. Set the autonomous system number.
 

```

[edit routing-options]
user@S-PE1# set autonomous-system 1

```
  3. Enable MPLS on all the interfaces of S-PE1 (ASBR 1), excluding the management interface.
 

```

[edit protocols]
user@S-PE1# set mpls interface all
user@S-PE1# set mpls interface fxp0.0 disable

```
  4. Enable autodiscovery of S-PE using BGP.
 

```

[edit protocols]
user@S-PE1# set bgp family l2vpn auto-discovery-mspw

```
  5. Configure the IBGP group for S-PE1 (ASBR 1) to peer with T-PE1.
 

```

[edit protocols]
user@S-PE1# set bgp group to_T-PE1 type internal

```
  6. Configure the IBGP group parameters.
 

```

[edit protocols]
user@S-PE1# set bgp group to_T-PE1 local-address 10.255.2.1
user@S-PE1# set bgp group to_T-PE1 export next-hop-self
user@S-PE1# set bgp group to_T-PE1 neighbor 10.255.10.1

```
  7. Configure the EBGp group for S-PE1 (ASBR 1) to peer with S-PE2 (ASBR 2).
 

```

[edit protocols]
user@S-PE1# set bgp group to_S-PE2 type external

```
  8. Configure the EBGp group parameters.
 

```

[edit protocols]
user@S-PE1# set bgp group to_S-PE2 local-address 10.255.2.1
user@S-PE1# set bgp group to_S-PE2 peer-as 2
user@S-PE1# set bgp group to_S-PE2 neighbor 10.255.3.1 multihop ttl 1

```
  9. Configure OSPF on all the interfaces of S-PE1 (ASBR 1), excluding the management interface.
 

```

[edit protocols]
user@S-PE1# set ospf area 0.0.0.0 interface all
user@S-PE1# set ospf area 0.0.0.0 interface fxp0.0 disable
user@S-PE1# set ospf area 0.0.0.0 interface lo0.0 passive

```
  10. Configure LDP on all the interfaces of S-PE1 (ASBR 1), excluding the management interface.
 

```

[edit protocols]
user@S-PE1# set ldp interface all
user@S-PE1# set ldp interface fxp0.0 disable
user@S-PE1# set ldp interface lo0.0

```
  11. Define the policy for enabling next-hop-self on S-PE1 (ASBR 1).
 

```

[edit policy-options]
user@S-PE1# set policy-statement next-hop-self then next-hop self

```

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

```
T-PE1 user@T-PE1# show interfaces
ge-3/1/0 {
 unit 0 {
 family inet {
 address 192.0.2.1/24;
 }
 family mpls;
 }
}
ge-3/1/2 {
 encapsulation ethernet-ccc;
 unit 0;
}
lo0 {
 unit 0 {
 family inet {
 address 10.255.10.1/32 {
 primary;
 }
 }
 }
}

user@T-PE1# show routing-options
autonomous-system 1;

user@T-PE1# show protocols
mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
}
bgp {
 family l2vpn {
 auto-discovery-mspw;
 }
 group mspw {
 type internal;
 local-address 10.255.10.1;
 neighbor 10.255.2.1;
 }
}
ospf {
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 interface lo0.0;
 }
}
```

```

}
ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 interface lo0.0;
}

user@T-PE1# show routing-instances
ms-pw {
 instance-type l2vpn;
 interface ge-3/1/2.0;
 route-distinguisher 10.10.10.10:15;
 l2vpn-id l2vpn-id:100:15;
 vrf-target target:100:115;
 protocols {
 l2vpn {
 site CE1 {
 source-attachment-identifier 800:800:800;
 interface ge-3/1/2.0 {
 target-attachment-identifier 700:700:700;
 }
 }
 pseudowire-status-tlv;
 oam {
 bfd-liveness-detection {
 minimum-interval 300;
 }
 }
 }
 }
}

S-PE1 (RR 1) user@S-PE1# show interfaces
ge-1/3/1 {
 unit 0 {
 family inet {
 address 192.0.2.9/24;
 }
 family mpls;
 }
}
ge-1/3/2 {
 unit 0 {
 family inet {
 address 192.0.2.12/24;
 }
 family mpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 10.255.2.1/32 {
 primary;
 }
 }
 }
}

```

```
 }
 }
}

user@T-PE1# show routing-options
autonomous-system 1;

user@S-PE1# show protocols
mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
}
bgp {
 family l2vpn {
 auto-discovery-mspw;
 }
 group to_T-PE1 {
 type internal;
 local-address 10.255.2.1;
 export next-hop-self;
 neighbor 10.255.10.1;
 }
 group to_S-PE2 {
 type external;
 local-address 10.255.2.1;
 peer-as 2;
 neighbor 10.255.3.1 {
 multihop {
 ttl 1;
 }
 }
 }
}
ospf {
 area 0.0.0.0 {
 interface lo0.0 {
 passive;
 }
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}
ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 interface lo0.0;
}

user@T-PE1# show policy-options
policy-statement next-hop-self {
```



```

 then {
 next-hop self;
 }
 }
}

```

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

## Verification

Confirm that the configuration is working properly.

- [Verifying the Routes on page 517](#)
- [Verifying the LDP Database on page 520](#)
- [Checking the MS-PW Connections on T-PE1 on page 521](#)
- [Checking the MS-PW Connections on S-PE1 on page 524](#)
- [Checking the MS-PW Connections on S-PE2 on page 527](#)
- [Checking the MS-PW Connections on T-PE2 on page 530](#)

### Verifying the Routes

**Purpose** Verify that the expected routes are learned.

**Action** From operational mode, run the **show route** command for the **bgp.l2vpn.1**, **ldp.l2vpn.1**, **mpls.0**, and **ms-pw.l2vpn.1** routing tables.

From operational mode, run the **show route table bgp.l2vpn.1** command.

```

user@T-PE1> show route table bgp.l2vpn.1
bgp.l2vpn.1: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.10.10.10:15:700:0.0.2.188:700/160 AD2
 *[BGP/170] 16:13:11, localpref 100, from 10.255.2.1
 AS path: 2 I, validation-state: unverified
 > to 192.0.2.2 via ge-3/1/0.0, Push 300016

```

From operational mode, run the **show route table ldp.l2vpn.1** command.

```

user@T-PE1> show route table ldp.l2vpn.1
ldp.l2vpn.1: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.255.2.1:CtrlWord:5:100:15:700:0.0.2.188:700:800:0.0.3.32:800/304 PW2
 *[LDP/9] 16:21:27
 Discard

```

From operational mode, run the **show route table mpls.0** command.

```

user@T-PE1> show route table mpls.0
mpls.0: 12 destinations, 12 routes (12 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0 *[MPLS/0] 1w6d 00:28:26, metric 1
 Receive
1 *[MPLS/0] 1w6d 00:28:26, metric 1

```

```

 Receive
2 *[MPLS/0] 1w6d 00:28:26, metric 1
 Receive
13 *[MPLS/0] 1w6d 00:28:26, metric 1
 Receive
299920 *[LDP/9] 1w5d 01:26:08, metric 1
 > to 192.0.2.2 via ge-3/1/0.0, Pop
299920(S=0) *[LDP/9] 1w5d 01:26:08, metric 1
 > to 192.0.2.2 via ge-3/1/0.0, Pop
299936 *[LDP/9] 1w5d 01:26:08, metric 1
 > to 192.0.2.2 via ge-3/1/0.0, Swap 300016
300096 *[LDP/9] 16:22:35, metric 1
 > to 192.0.2.2 via ge-3/1/0.0, Swap 300128
300112 *[LDP/9] 16:22:35, metric 1
 > to 192.0.2.2 via ge-3/1/0.0, Swap 300144
300128 *[LDP/9] 16:22:35, metric 1
 > to 192.0.2.2 via ge-3/1/0.0, Swap 300160
300144 *[L2VPN/7] 16:22:33
 > via ge-3/1/2.0, Pop Offset: 4
ge-3/1/2.0 *[L2VPN/7] 16:22:33, metric2 1
 > to 192.0.2.2 via ge-3/1/0.0, Push 300176, Push 300016(top)
Offset: 252

```

From operational mode, run the **show route table ms-pw.l2vpn.1** command.

```

user@T-PE1> show route table ms-pw.l2vpn.1
ms-pw.l2vpn.1: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.10.10.10:15:700:0.0.2.188:700/160 AD2
 *[BGP/170] 16:23:27, localpref 100, from 10.255.2.1
 AS path: 2 I, validation-state: unverified
 > to 192.0.2.2 via ge-3/1/0.0, Push 300016
10.10.10.10:15:800:0.0.3.32:800/160 AD2
 *[L2VPN/170] 1w5d 23:25:19, metric2 1
 Indirect
10.255.2.1:CtrlWord:5:100:15:700:0.0.2.188:700:800:0.0.3.32:800/304 PW2
 *[LDP/9] 16:23:25
 Discard
10.255.2.1:CtrlWord:5:100:15:800:0.0.3.32:800:700:0.0.2.188:700/304 PW2
 *[L2VPN/7] 16:23:27, metric2 1
 > to 192.0.2.2 via ge-3/1/0.0, Push 300016

```

**Meaning** The output shows all the learned routes, including the autodiscovery (AD) routes.

The AD2 prefix format is **RD:SAII-type2**, where:

- **RD** is the route distinguisher value.
- **SAII-type2** is the type 2 source attachment identifier value.

The PW2 prefix format is **Neighbor\_Addr:C:PWtype:l2vpn-id:SAII-type2:TAII-type2**, where:

- **Neighbor\_Addr** is the loopback address of neighboring S-PE device.
- **C** indicates if Control Word (CW) is enabled or not.
  - **C** is **CtrlWord** if CW is set.

- **C** is **NoCtrlWord** if CW is not set.
- **PWtype** indicates the type of the pseudowire.
  - **PWtype** is **4** if it is in Ethernet tagged mode.
  - **PWtype** is **5** if it is Ethernet only.
- **l2vpn-id** is the Layer 2 VPN ID for the MS-PW routing instance.
- **SAll-type2** is the type 2 source attachment identifier value.
- **TAll-type2** is the type 2 target attachment identifier value.

## Verifying the LDP Database

**Purpose** Verify the MS-PW labels received by T-PE1 from S-PE1 and sent from T-PE1 to S-PE1.

**Action** From operational mode, run the **show ldp database** command.

```
user@T-PE1> show ldp database
Input label database, 10.255.10.1:0--10.255.2.1:0
 Label Prefix
 3 10.255.2.1/32
 300112 10.255.3.1/32
 300128 10.255.4.1/32
 299968 10.255.10.1/32
 299904 10.255.13.1/32
 300144 10.255.14.1/32
 300176 FEC129 CtrlWord ETHERNET 000a0064:0000000f 000002bc:000002bc:000002bc
00000320:00000320:00000320
```

```
Output label database, 10.255.10.1:0--10.255.2.1:0
 Label Prefix
 299936 10.255.2.1/32
 300096 10.255.3.1/32
 300112 10.255.4.1/32
 3 10.255.10.1/32
 299920 10.255.13.1/32
 300128 10.255.14.1/32
 300144 FEC129 CtrlWord ETHERNET 000a0064:0000000f
00000320:00000320:00000320 000002bc:000002bc:000002bc
```

```
Input label database, 10.255.10.1:0--10.255.13.1:0
 Label Prefix
 300016 10.255.2.1/32
 300128 10.255.3.1/32
 300144 10.255.4.1/32
 300080 10.255.10.1/32
 3 10.255.13.1/32
 300160 10.255.14.1/32
```

```
Output label database, 10.255.10.1:0--10.255.13.1:0
 Label Prefix
 299936 10.255.2.1/32
 300096 10.255.3.1/32
 300112 10.255.4.1/32
 3 10.255.10.1/32
 299920 10.255.13.1/32
 300128 10.255.14.1/32
```

**Meaning** The labels with **FEC129** prefix are related to the MS-PW.

### Checking the MS-PW Connections on T-PE1

**Purpose** Make sure that all of the FEC 129 MS-PW connections come up correctly.

**Action** From operational mode, run the **show l2vpn connections extensive** command.

```
user@T-PE1> show l2vpn connections extensive
```

```
Layer-2 VPN connections:
```

```
Legend for connection status (St)
```

```

EI -- encapsulation invalid NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down NP -- interface hardware not present
CM -- control-word mismatch -> -- only outbound connection is up
CN -- circuit not provisioned <- -- only inbound connection is up
OR -- out of range Up -- operational
OL -- no outgoing label Dn -- down
LD -- local site signaled down CF -- call admission control failure
RD -- remote site signaled down SC -- local and remote site ID collision
LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status IL -- no incoming label
MM -- MTU mismatch MI -- Mesh-Group ID not available
BK -- Backup connection ST -- Standby connection
PF -- Profile parse failure PB -- Profile busy
RS -- remote site standby SN -- Static Neighbor
LB -- Local site not best-site RB -- Remote site not best-site
VM -- VLAN ID mismatch

```

```
Legend for interface status
```

```

Up -- operational
Dn -- down

```

```
Instance: ms-pw
```

```
L2vpn-id: 100:15
```

```
Number of local interfaces: 1
```

```
Number of local interfaces up: 1
```

```
ge-3/1/2.0
```

```
Local source-attachment-id: 800:0.0.3.32:800 (CE1)
```

| Target-attachment-id | Type | St | Time last up         | # Up trans |
|----------------------|------|----|----------------------|------------|
| 700:0.0.2.188:700    | rmt  | Up | Sep 18 01:10:55 2013 | 1          |

```
Remote PE: 10.255.2.1, Negotiated control-word: Yes (Null)
```

```
Incoming label: 300048, Outgoing label: 300016
```

```
Negotiated PW status TLV: Yes
```

```
Local PW status code: 0x00000000, Neighbor PW status code: 0x00000000
```

```
Local interface: ge-3/1/2.0, Status: Up, Encapsulation: ETHERNET
```

```
Pseudowire Switching Points :
```

| Local address | Remote address | Status     |
|---------------|----------------|------------|
| 10.255.2.1    | 10.255.3.1     | forwarding |
| 10.255.3.1    | 10.255.14.1    | forwarding |

```
Connection History:
```

|                      |                     |            |
|----------------------|---------------------|------------|
| Sep 18 01:10:55 2013 | status update timer |            |
| Sep 18 01:10:55 2013 | PE route changed    |            |
| Sep 18 01:10:55 2013 | Out lbl Update      | 300016     |
| Sep 18 01:10:55 2013 | In lbl Update       | 300048     |
| Sep 18 01:10:55 2013 | loc intf up         | ge-3/1/2.0 |

Check the following fields in the output to verify that MS-PW is established between the T-PE devices:

- **Target-attachment-id**—Check if the TAI value is the SAI value of T-PE2.
- **Remote PE**—Check if the T-PE2 loopback address is listed.

- **Negotiated PW status TLV**—Ensure that the value is **Yes**.
- **Pseudowire Switching Points**—Check if the switching points are listed from S-PE1 to S-PE2 and from S-PE2 to T-PE2.

**Meaning** MS-PW is established between T-PE1 and T-PE2 in the forwarding direction.

### Checking the MS-PW Connections on S-PE1

**Purpose** Make sure that all of the FEC 129 MS-PW connections come up correctly for the mspw routing instance.



**Action** From operational mode, run the **show l2vpn connections instance \_\_MSPW\_\_ extensive** command.

```
user@S-PE1> show l2vpn connections instance __MSPW__ extensive
```

Layer-2 VPN connections:

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -> -- only outbound connection is up           |
| CN -- circuit not provisioned    | <- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unknown connection status  | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not available              |
| BK -- Backup connection          | ST -- Standby connection                       |
| PF -- Profile parse failure      | PB -- Profile busy                             |
| RS -- remote site standby        | SN -- Static Neighbor                          |
| LB -- Local site not best-site   | RB -- Remote site not best-site                |
| VM -- VLAN ID mismatch           |                                                |

Legend for interface status

Up -- operational  
Dn -- down

Instance: \_\_MSPW\_\_

L2vpn-id: 100:15

Local source-attachment-id: 700:0.0.2.188:700

| Target-attachment-id | Type | St | Time last up         | # Up trans |
|----------------------|------|----|----------------------|------------|
| 800:0.0.3.32:800     | rmt  | Up | Sep 18 01:17:38 2013 | 1          |

Remote PE: 10.255.10.1, Negotiated control-word: Yes (Null), Encapsulation:

ETHERNET

Incoming label: 300016, Outgoing label: 300048

Negotiated PW status TLV: Yes

local PW status code: 0x00000000, Neighbor PW status code: 0x00000000

Local source-attachment-id: 800:0.0.3.32:800

| Target-attachment-id | Type | St | Time last up         | # Up trans |
|----------------------|------|----|----------------------|------------|
| 700:0.0.2.188:700    | rmt  | Up | Sep 18 01:17:38 2013 | 1          |

Remote PE: 10.255.3.1, Negotiated control-word: Yes (Null), Encapsulation:

ETHERNET

Incoming label: 300000, Outgoing label: 300064

Negotiated PW status TLV: Yes

local PW status code: 0x00000000, Neighbor PW status code: 0x00000000

Pseudowire Switching Points :

| Local address | Remote address | Status     |
|---------------|----------------|------------|
| 10.255.3.1    | 10.255.14.1    | forwarding |

Check the following fields in the output to verify that MS-PW is established between the T-PE devices:

- **Target-attachment-id**—Check if the TAI value is the SAI value of T-PE2.
- **Remote PE**—Check if the T-PE1 and S-PE2 loopback addresses are listed.
- **Negotiated PW status TLV**—Ensure that the value is **Yes**.

- **Pseudowire Switching Points**—Check if the switching points are listed from S-PE2 to T-PE2.

**Meaning** MS-PW is established between T-PE1 and T-PE2 in the forwarding direction.

### Checking the MS-PW Connections on S-PE2

**Purpose** Make sure that all of the FEC 129 MS-PW connections come up correctly for the mspw routing instance.

**Action** From operational mode, run the **show l2vpn connections instance\_\_MSPW\_\_ extensive** command.

```
user@S-PE2> show l2vpn connections instance__MSPW__ extensive
Layer-2 VPN connections:
```

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -> -- only outbound connection is up           |
| CN -- circuit not provisioned    | <- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unknown connection status  | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not available              |
| BK -- Backup connection          | ST -- Standby connection                       |
| PF -- Profile parse failure      | PB -- Profile busy                             |
| RS -- remote site standby        | SN -- Static Neighbor                          |
| LB -- Local site not best-site   | RB -- Remote site not best-site                |
| VM -- VLAN ID mismatch           |                                                |

Legend for interface status

Up -- operational  
Dn -- down

Instance: \_\_MSPW\_\_

L2vpn-id: 100:15

Local source-attachment-id: 700:0.0.2.188:700

| Target-attachment-id | Type | St | Time last up         | # Up trans |
|----------------------|------|----|----------------------|------------|
| 800:0.0.3.32:800     | rmt  | Up | Sep 18 00:58:55 2013 | 1          |

Remote PE: 10.255.2.1, Negotiated control-word: Yes (Null), Encapsulation:

ETHERNET

Incoming label: 300064, Outgoing label: 300000

Negotiated PW status TLV: Yes

local PW status code: 0x00000000, Neighbor PW status code: 0x00000000

Pseudowire Switching Points :

| Local address | Remote address | Status     |
|---------------|----------------|------------|
| 10.255.2.1    | 10.255.10.1    | forwarding |

Local source-attachment-id: 800:0.0.3.32:800

| Target-attachment-id | Type | St | Time last up         | # Up trans |
|----------------------|------|----|----------------------|------------|
| 700:0.0.2.188:700    | rmt  | Up | Sep 18 00:58:55 2013 | 1          |

Remote PE: 10.255.14.1, Negotiated control-word: Yes (Null), Encapsulation:

ETHERNET

Incoming label: 300048, Outgoing label: 300112

Negotiated PW status TLV: Yes

local PW status code: 0x00000000, Neighbor PW status code: 0x00000000

Check the following fields in the output to verify that MS-PW is established between the T-PE devices:

- **Target-attachment-id**—Check if the TAI value is the SAI value of T-PE1.
- **Remote PE**—Check if the S-PE1 and T-PE2 loopback addresses are listed.
- **Negotiated PW status TLV**—Ensure that the value is **Yes**.

- **Pseudowire Switching Points**—Check if the switching points are listed from S-PE1 to T-PE1.

**Meaning** MS-PW is established between T-PE1 and T-PE2 in the reverse direction.

### Checking the MS-PW Connections on T-PE2

---

**Purpose** Make sure that all of the FEC 129 MS-PW connections come up correctly.

**Action** From operational mode, run the **show l2vpn connections extensive** command.

```
user@T-PE2> show l2vpn connections extensive
Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down NP -- interface hardware not present
CM -- control-word mismatch -> -- only outbound connection is up
CN -- circuit not provisioned <- -- only inbound connection is up
OR -- out of range Up -- operational
OL -- no outgoing label Dn -- down
LD -- local site signaled down CF -- call admission control failure
RD -- remote site signaled down SC -- local and remote site ID collision
LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status IL -- no incoming label
MM -- MTU mismatch MI -- Mesh-Group ID not available
BK -- Backup connection ST -- Standby connection
PF -- Profile parse failure PB -- Profile busy
RS -- remote site standby SN -- Static Neighbor
LB -- Local site not best-site RB -- Remote site not best-site
VM -- VLAN ID mismatch

Legend for interface status
Up -- operational
Dn -- down

Instance: ms-pw
L2vpn-id: 100:15
 Number of local interfaces: 1
 Number of local interfaces up: 1
 ge-2/0/0.0
Local source-attachment-id: 700:0.0.2.188:700 (CE2)
 Target-attachment-id Type St Time last up # Up trans
 800:0.0.3.32:800 rmt Up Sep 18 01:35:21 2013 1
 Remote PE: 10.255.3.1, Negotiated control-word: Yes (Null)
 Incoming label: 300112, Outgoing label: 300048
 Negotiated PW status TLV: Yes
 Local PW status code: 0x00000000, Neighbor PW status code: 0x00000000
 Local interface: ge-2/0/0.0, Status: Up, Encapsulation: ETHERNET
 Pseudowire Switching Points :
 Local address Remote address Status
 10.255.3.1 10.255.2.1 forwarding
 10.255.2.1 10.255.10.1 forwarding
 Connection History:
 Sep 18 01:35:21 2013 status update timer
 Sep 18 01:35:21 2013 PE route changed
 Sep 18 01:35:21 2013 Out lbl Update 300048
 Sep 18 01:35:21 2013 In lbl Update 300112
 Sep 18 01:35:21 2013 loc intf up ge-2/0/0.0
```

Check the following fields in the output to verify that MS-PW is established between the T-PE devices:

- **Target-attachment-id**—Check if the TAI value is the SAI value of T-PE1.
- **Remote PE**—Check if the T-PE1 loopback address is listed.

- **Negotiated PW status TLV**—Ensure that the value is **Yes**.
- **Pseudowire Switching Points**—Check if the switching points are listed from S-PE2 to S-PE1 and from S-PE1 to T-PE1.

**Meaning** MS-PW is established between T-PE1 and T-PE2 in the reverse direction.

## Troubleshooting

To troubleshoot the MS-PW connection, see:

- [Ping on page 532](#)
- [Bidirectional Forwarding Detection on page 532](#)
- [Traceroute on page 533](#)

### Ping

**Problem** How to check the connectivity between the T-PE devices and between a T-PE device and an intermediary device.

**Solution** Verify that T-PE1 can ping T-PE2. The **ping mpls l2vpn fec129** command accepts SAls and TAls as integers or IP addresses and also allows you to use the CE-facing interface instead of the other parameters (**instance**, **local-id**, **remote-id**, **remote-pe-address**).

#### Checking Connectivity Between T-PE1 and T-PE2

```
user@T-PE1> ping mpls l2vpn fec129 instance FEC129-VPWS local-id 800:800:800
remote-pe-address 10.255.14.1 remote-id 700:700:700
!!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss

user@T-PE1> ping mpls l2vpn fec129 interface ge-3/1/2
!!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

#### Checking Connectivity Between T-PE1 and S-PE2

```
user@T-PE1> ping mpls l2vpn fec129 interface ge-3/1/2 bottom-label-ttl 2
!!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

### Bidirectional Forwarding Detection

**Problem** How to use BFD to troubleshoot the MS-PW connection from the T-PE device.

**Solution** From operational mode, verify the **show bfd session extensive** command output.

```
user@T-PE1> show bfd session extensive
```

| Address      | State | Interface  | Detect Time | Transmit Interval | Multiplier |
|--------------|-------|------------|-------------|-------------------|------------|
| 198.51.100.1 | Up    | ge-3/1/0.0 | 0.900       | 0.300             | 3          |



```

Client FEC129-OAM, TX interval 0.300, RX interval 0.300
Session up time 03:12:42
Local diagnostic None, remote diagnostic None
Remote state Up, version 1
Replicated
Session type: VCCV BFD
Min async interval 0.300, min slow interval 1.000
Adaptive async TX interval 0.300, RX interval 0.300
Local min TX interval 0.300, minimum RX interval 0.300, multiplier 3
Remote min TX interval 0.300, min RX interval 0.300, multiplier 3
Local discriminator 19, remote discriminator 19
Echo mode disabled/inactive
Remote is control-plane independent
L2vpn-id 100:15, Local-id 800:0.0.3.32:800, Remote-id 700:0.0.2.188:700
Session ID: 0x103

```

1 sessions, 1 clients

Cumulative transmit rate 3.3 pps, cumulative receive rate 3.3 pps

### Traceroute

**Problem** How to verify that MS-PW was established.

**Solution** From operational mode, verify **traceroute** output.

```

user@T-PE1> traceroute mpls l2vpn fec129 interface interface
Probe options: ttl 64, retries 3, exp 7

```

| ttl | Label | Protocol | Address     | Previous Hop | Probe Status |
|-----|-------|----------|-------------|--------------|--------------|
| 1   |       | FEC129   | 10.255.10.1 | (null)       | Success      |
| 2   |       | FEC129   | 10.255.2.1  | 10.255.10.1  | Success      |
| 3   |       | FEC129   | 10.255.3.1  | 10.255.2.1   | Success      |
| 4   |       | FEC129   | 10.255.14.1 | 10.255.2.1   | Egress       |

Path 1 via ge-3/1/2 destination 127.0.0.0

**Related Documentation**

- [Understanding Multisegment Pseudowire for FEC 129 on page 451](#)

## Configuring the FAT Flow Label for FEC 128 VPWS Pseudowires for Load-Balancing MPLS Traffic

---

This topic shows how to configure flow-aware transport of pseudowires (FAT) flow labels for forwarding equivalence class (FEC) 128 virtual private wire service (VPWS) pseudowires for load-balancing MPLS traffic.

FAT flow labels enable load-balancing of MPLS packets across equal-cost multipath (ECMP) paths or link aggregation groups (LAGs) without the need for deep packet inspection of the payload. FAT flow labels can be used for LDP-signaled FEC 128 and FEC 129 pseudowires for virtual private LAN service (VPLS) and VPWS networks.

You can configure FAT flow labels to be signaled by LDP on FEC 128 VPWS pseudowires by including the **flow-label-transmit** and **flow-label-receive** configuration statements at the `[edit protocols l2circuit neighbor neighbor-id interface interface-name]` hierarchy level. This configuration sets the T bit and R bit advertisement to 1 (the default being 0) in the Sub-TLV field, which is one of the interface parameters of the FEC for the LDP label-mapping message header. These statements signal the pushing and popping of the load-balancing label to the routing peers in the control plane.

Alternatively, you can configure the following statements at the `[edit protocols l2circuit neighbor neighbor-id interface interface-name]` hierarchy level:

- **flow-label-transmit-static** to statically push the flow label on the pseudowire packets sent to the remote provider edge (PE) router.
- **flow-label-receive-static** to statically pop the flow label on the pseudowire packets received from the remote PE router.

Before you begin:

1. Configure the device interfaces and enable MPLS on all the interfaces.
2. Configure MPLS and an LSP to the remote PE router.
3. Configure OSPF and IS-IS.
4. Configure LDP on the loopback interface and the PE interface connecting to the P (transit) router.

To configure the FAT flow label for an FEC 128-signaled VPLS pseudowire, on the ingress PE router:

1. Configure the neighbors for the Layer 2 circuit.

```
[edit protocols l2circuit]
user@PE1# set neighbor neighbor-id
```

All the Layer 2 circuits using a particular remote PE router designated for remote CE routers are listed under the **neighbor** statement. Each neighbor is identified by its IP address and is usually the end-point destination for the label-switched path (LSP) tunnel transporting the Layer 2 circuit.

2. Configure the interface for the Layer 2 circuit neighbor and a unique identifier for the Layer 2 circuit.

```
[edit protocols l2circuit neighbor neighbor-id]
user@PE1# set interface interface-name virtual-circuit-id unique-l2ckt-identifier
```

- 3.



**NOTE:** You can only configure one of the following pairs of statements:

- **flow-label-transmit** and **flow-label-receive** or,
- **flow-label-transmit-static** and **flow-label-receive-static**

Configure the router to signal the capability to push the flow label in the transmit direction to the remote PE router.

```
[edit protocols l2circuit neighbor neighbor-id interface interface-name]
user@PE1# set flow-label-transmit
```

4. Alternatively, configure the **flow-label-transmit-static** statement to statically push the flow label on the pseudowire packets sent to the remote PE router.

```
[edit protocols l2circuit neighbor neighbor-id interface interface-name]
user@PE1# set flow-label-transmit-static
```

If the incoming pseudowire packet is not marked with the flow label, the packet is dropped by the egress PE router.

5. Configure the router to signal the capability to pop the flow label in the receive direction to the remote egress PE router.

```
[edit protocols l2circuit neighbor neighbor-id interface interface-name]
user@PE1# set flow-label-receive
```

6. Alternatively, configure the **flow-label-receive-static** statement to pop the flow label on the pseudowire packets received from the remote PE router.

```
[edit protocols l2circuit neighbor neighbor-id interface interface-name]
user@PE1# set flow-label-receive-static
```

The ingress PE router inserts the flow label in the pseudowire packet, irrespective of the information exchanged in the signaling plane. If the egress PE router cannot handle the pseudowire packet marked with the flow label, the packet is dropped.

7. Verify and commit the configuration.

For example:

```
[edit protocols l2circuit]
user@PE1# show
neighbor 10.255.104.135 {
 interface ge-1/0/8.0 {
 virtual-circuit-id 1;
 flow-label-transmit;
 flow-label-receive;
 }
}
```

OR:

```
[edit protocols l2circuit]
user@PE1# show
neighbor 10.255.104.135 {
 interface ge-1/0/8.0 {
 virtual-circuit-id 1;
 flow-label-transmit-static;
 flow-label-receive-static;
 }
}
```

8. Repeat the configuration on the remote egress PE router.

**Related Documentation**

- [Configuring the FAT Flow Label for FEC 128 VPLS Pseudowires for Load-Balancing MPLS Traffic on page 629](#)
- [Configuring the FAT Flow Label for FEC 129 VPWS Pseudowires for Load-Balancing MPLS Traffic on page 536](#)
- [Configuring the FAT Flow Label for FEC 129 VPLS Pseudowires for Load-Balancing MPLS Traffic on page 631](#)
- *FAT Flow Labels Overview*

---

## Configuring the FAT Flow Label for FEC 129 VPWS Pseudowires for Load-Balancing MPLS Traffic

---

This topic shows how to configure flow-aware transport of pseudowires (FAT) flow labels for forwarding equivalence class (FEC) 129 virtual private wire service (VPWS) pseudowires.

FAT flow labels enable load-balancing of MPLS packets across equal-cost multipath (ECMP) paths or link aggregation groups (LAGs) without the need for deep packet inspection of the payload. FAT flow labels can be used for LDP-signaled FEC 128 and FEC 129 pseudowires for virtual private LAN service (VPLS) and VPWS networks.

You can configure FAT flow labels to be signaled by LDP on FEC 129 VPWS pseudowires (Layer 2 circuits) by including the **flow-label-transmit** and **flow-label-receive** configuration statements at the **[edit routing-instances *instance-name* protocols l2vpn site *name*]** or the **[edit routing-instances *instance-name* protocols l2vpn site *name* interface *interface-name*]** hierarchy level. This configuration sets the T bit and R bit advertisement to 1 (the default being 0) in the Sub-TLV field, which is one of the interface parameters of the FEC for the LDP label-mapping message header. These statements signal the pushing and popping of the load-balancing label to the routing peers in the control plane.

Before you begin:

1. Configure the device interfaces and enable MPLS on all core-facing interfaces.
2. Configure CCC encapsulation and the CCC address family for interfaces configured as members of the FEC 129 VPWS instance.
3. Configure MPLS and an LSP to the remote provider edge (PE) router.

4. Configure the BGP sessions on the PE devices with the BGP autodiscovery-only address family to allow exchange of the autodiscovery routes.
5. Configure an IGP such as IS-IS or OSPF.
6. Configure LDP on the loopback interface and the core-facing interface.
7. Configure the autonomous system (AS) number.

To configure the FAT flow label for an FEC 129 VPWS pseudowire, on the ingress PE router:

1. Configure the VPWS routing instance.

LDP listens for routes from instance.l2vpn.0 for any instance configured for FEC 129 VPWS. These routes are identified by the **instance-type l2vpn** statement in the routing instance and the presence of the **l2vpn-id** statement.

```
[edit]
user@PE1# set routing-instances instance-name instance-type l2vpn
user@PE1# set routing-instances instance-name interface interface-name
user@PE1# set routing-instances instance-name route-distinguisher (as-number:x:y
| ip-address:id)
user@PE1# set routing-instances instance-name l2vpn-id (as-number:x:y | ip-address:id)
user@PE1# set routing-instances instance-name vrf-target community
user@PE1# set routing-instances instance-name protocols l2vpn site site-name
source-attachment-identifier identifier
user@PE1# set routing-instances instance-name protocols l2vpn site site-name
interface interface-name target-attachment-identifier identifier
```

Because VPWS is a point-to-point service, FEC 129 VPWS routing instances are configured as **instance-type l2vpn**. As with FEC 129 VPLS, FEC 129 VPWS uses the **l2vpn-id** statement to define the Layer 2 VPN of which the routing instance is a member. The presence of the **l2vpn-id** statement designates that FEC 129 LDP-signaling is used for the routing instance.

2. Configure the device to signal the capability to push the flow label in the transmit direction to the remote PE router.

```
[edit routing-instances instance-name protocols l2vpn site name interface
interface-name]
user@PE1# set flow-label-transmit
```

3. Configure the device to signal the capability to pop the flow label in the receive direction to the remote PE router.

```
[edit routing-instances instance-name protocols l2vpn site name interface
interface-name]
user@PE1# set flow-label-receive
```

4. Alternatively, configure the **flow-label-transmit** and **flow-label-receive** statements directly within the site. When configured within the site, the defined parameters affect any pseudowire originating from that site. When configured under an interface within the site, the defined parameters affect that single specific pseudowire. This enables you to manipulate the parameters across all pseudowires associated with a particular local site in one place in the configuration.

```
[edit routing-instances instance-name protocols l2vpn site name]
```

```

user@PE1# set flow-label-receive
user@PE1# set flow-label-transmit

```

5. Verify and commit the configuration.

For example:

```

[edit routing-instances FEC129-VPWS]
user@PE1# show
instance-type l2vpn;
interface ge-0/0/1.600;
route-distinguisher 10.255.255.1:100;
l2vpn-id l2vpn-id:100:100;
vrf-target target:100:100;
protocols {
 l2vpn {
 site ONE {
 source-attachment-identifier 1;
 interface ge-0/0/1.600 {
 target-attachment-identifier 2;
 flow-label-transmit; <<< Applicable only to the pseudowire specific to the
 interface >>>
 flow-label-receive;
 }
 }
 site TWO {
 source-attachment-identifier 3;
 flow-label-transmit; <<< Applicable to all pseudowires within the site >>>
 flow-label-receive;
 interface ge-0/0/2.600 {
 target-attachment-identifier 1;
 }
 interface ge-0/0/2.601 {
 target-attachment-identifier 4;
 }
 }
 }
}

```

6. Repeat the configuration on the remote egress PE router.

#### Related Documentation

- [Configuring the FAT Flow Label for FEC 128 VPWS Pseudowires for Load-Balancing MPLS Traffic on page 534](#)
- [Configuring the FAT Flow Label for FEC 128 VPLS Pseudowires for Load-Balancing MPLS Traffic on page 629](#)
- [Configuring the FAT Flow Label for FEC 129 VPLS Pseudowires for Load-Balancing MPLS Traffic on page 631](#)
- *FAT Flow Labels Overview*

## PART 7

# Configuring VPLS

- [Overview on page 541](#)
- [VPLS Configuration Overview on page 545](#)
- [Configuring Signaling Protocols for VPLS on page 547](#)
- [Assigning Routing Instances to VPLS on page 563](#)
- [Associating Interfaces with VPLS on page 603](#)
- [Configuring Pseudowires on page 613](#)
- [Configuring Multihoming on page 705](#)
- [Configuring Point-to-Multipoint LSPs on page 809](#)
- [Configuring Inter-AS VPLS and IRB VPLS on page 867](#)
- [Configuring Load Balancing and Performance on page 895](#)
- [Configuring Class of Service and Firewall Filters in VPLS on page 921](#)
- [Monitoring and Tracing VPLS on page 939](#)





# Overview

- [Introduction to VPLS on page 541](#)
- [Supported VPLS Standards on page 542](#)
- [Supported Platforms and PICs on page 542](#)

## Introduction to VPLS

---

VPLS is an Ethernet-based point-to-multipoint Layer 2 VPN. It allows you to connect geographically dispersed Ethernet local area networks (LAN) sites to each other across an MPLS backbone. For customers who implement VPLS, all sites appear to be in the same Ethernet LAN even though traffic travels across the service provider's network.

VPLS, in its implementation and configuration, has much in common with a Layer 2 VPN. In VPLS, a packet originating within a service provider customer's network is sent first to a customer edge (CE) device (for example, a router or Ethernet switch). It is then sent to a provider edge (PE) router within the service provider's network. The packet traverses the service provider's network over a MPLS label-switched path (LSP). It arrives at the egress PE router, which then forwards the traffic to the CE device at the destination customer site.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

The difference is that for VPLS, packets can traverse the service provider's network in point-to-multipoint fashion, meaning that a packet originating from a CE device can be broadcast to all the PE routers participating in a VPLS routing instance. In contrast, a Layer 2 VPN forwards packets in point-to-point fashion only.

The paths carrying VPLS traffic between each PE router participating in a routing instance are called pseudowires. The pseudowires are signaled using either BGP or LDP.

## Supported VPLS Standards

---

Junos OS substantially supports the following Internet RFCs and draft, which define standards for virtual private LAN service (VPLS).

- RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*
- RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*

FEC 128, FEC 129, control bit 0, the Ethernet pseudowire type 0x0005, and the Ethernet tagged mode pseudowire type 0x0004 are supported.

- RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*
- RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*
- Internet draft draft-kompella-l2vpn-vpls-multihoming, *Multi-homing in BGP-based Virtual Private LAN Service*

### Related Documentation

- *Supported Carrier-of-Carriers and Interprovider VPN Standards*
- [Supported VPWS Standards on page 450](#)
- [Supported Layer 2 VPN Standards on page 123](#)
- *Supported Layer 3 VPN Standards*
- *Supported Multicast VPN Standards*
- *Accessing Standards Documents on the Internet*

## Supported Platforms and PICs

---

Virtual private LAN service (VPLS) is supported on all M Series routers except the M160.

VPLS is supported on all MX Series and T Series routers.

VPLS is supported on the following SRX Services Gateways for the branch:

- SRX100
- SRX210
- SRX240
- SRX650

VPLS is supported on the following PICs:

- All ATM2 IQ PICs
- 4-port Fast Ethernet PIC with 10/100 Base-TX interfaces PIC
- 1-port, 2-port, and 10-port Gigabit Ethernet PICs
- 1-port, 2-port, and 4-port Gigabit Ethernet PICs with SFP

- 1-port 10-Gigabit Ethernet PIC
- 1-port and 2-port Gigabit Ethernet Intelligent Queuing (IQ) PICs
- 4-port and 8-port Gigabit Ethernet IQ2 PICs with SFP
- 1-port 10-Gigabit Ethernet IQ2 PIC with XFP
- 4-port, quad-wide Gigabit Ethernet PIC
- 10-port 10-Gigabit OSE PIC



# VPLS Configuration Overview

- [Introduction to Configuring VPLS on page 545](#)
- [Configuring an Ethernet Switch as the CE Device for VPLS on page 545](#)

## Introduction to Configuring VPLS

---

Virtual private LAN service (VPLS) allows you to provide a point-to-multipoint LAN between a set of sites in a virtual private network (VPN).

To configure VPLS functionality, you must enable VPLS support on the provider edge (PE) router. You must also configure PE routers to distribute routing information to the other PE routers in the VPLS and configure the circuits between the PE routers and the customer edge (CE) routers.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

Each VPLS is configured under a routing instance of type **vpls**. A **vpls** routing instance can transparently carry Ethernet traffic across the service provider's network. As with other routing instances, all logical interfaces belonging to a VPLS routing instance are listed under that instance.

In addition to VPLS routing instance configuration, you must configure MPLS label-switched paths (LSPs) between the PE routers, IBGP sessions between the PE routers, and an interior gateway protocol (IGP) on the PE and provider (P) routers.

By default, VPLS is disabled.

Many configuration procedures for VPLS are identical to the procedures for Layer 2 VPNs and Layer 3 VPNs.

## Configuring an Ethernet Switch as the CE Device for VPLS

---

For VPLS configurations, the CE device does not necessarily need to be a router. You can link the PE routers directly to Ethernet switches. However, there are a few configuration issues to be aware of:

- When you configure VPLS routing instances and establish two or more connections between a CE Ethernet switch and a PE router, you must enable the Spanning Tree Protocol (STP) on the switch to prevent loops.
- The Junos OS allows standard Bridge Protocol Data Unit (BPDU) frames to pass through emulated Layer 2 connections, such as those configured with Layer 2 VPNs, Layer 2 circuits, and VPLS instances. However, CE Ethernet switches that generate proprietary BPDU frames might not be able to run STP across Juniper Networks routing platforms configured for these emulated Layer 2 connections.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

# Configuring Signaling Protocols for VPLS

- [VPLS Routing and Virtual Ports on page 547](#)
- [BGP Signaling for VPLS PE Routers Overview on page 549](#)
- [Control Word for BGP VPLS Overview on page 550](#)
- [Configuring a Control Word for BGP VPLS on page 551](#)
- [BGP Route Reflectors for VPLS on page 552](#)
- [Interoperability Between BGP Signaling and LDP Signaling in VPLS on page 554](#)
- [Configuring Interoperability Between BGP Signaling and LDP Signaling in VPLS on page 556](#)

## VPLS Routing and Virtual Ports

---

Because VPLS carries Ethernet traffic across a service provider network, it must mimic an Ethernet network in some ways. When a PE router configured with a VPLS routing instance receives a packet from a CE device, it first determines whether it has the destination of the VPLS packet in the appropriate routing table. If it does, it forwards the packet to the appropriate PE router or CE device. If it does not, it broadcasts the packet to all other PE routers and CE devices that are members of that VPLS routing instance. In both cases, the CE device receiving the packet must be different from the one sending the packet.



**NOTE:** In the VPLS documentation, the term *router* is used to refer to any device that provides routing functions.

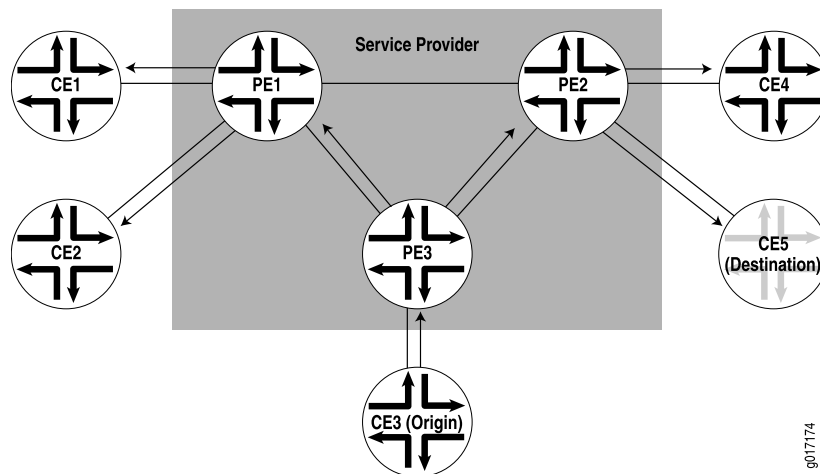
When a PE router receives a packet from another PE router, it first determines whether it has the destination of the VPLS packet in the appropriate routing table. If it does, the PE router either forwards the packet or drops it depending on whether the destination is a local or remote CE device:

- If the destination is a local CE device, the PE router forwards the packet to it.
- If the destination is a remote CE device (connected to another PE router), the PE router discards the packet.

If the PE router cannot determine the destination of the VPLS packet, it floods the packet to all attached CE devices.

This process is illustrated in [Figure 48 on page 548](#).

**Figure 48: Flooding a Packet with an Unknown Destination to All PE Routers in the VPLS Instance**



VPLS can be directly connected to an Ethernet switch. Layer 2 information gathered by an Ethernet switch (for example, media access control [MAC] addresses and interface ports) is included in the VPLS routing instance table. However, instead of all VPLS interfaces being physical switch ports, the router allows remote traffic for a VPLS instance to be delivered across an MPLS LSP and arrive on a virtual port. The virtual port emulates a local, physical port. Traffic can be learned, forwarded, or flooded to the virtual port in almost the same way as traffic is sent to a local port.

The VPLS routing table learns MAC address and interface information for both physical and virtual ports. The main difference between a physical port and a virtual port is that the router captures additional information from the virtual port, an outgoing MPLS label used to reach the remote site and an incoming MPLS label for VPLS traffic received from the remote site. The virtual port is generated dynamically on a Tunnel Services Physical Interface Card (PIC) when you configure VPLS on the router.

You can also configure VPLS without a Tunnel Services PIC. To do so, you use a label-switched interface (LSI) to provide VPLS functionality. An LSI MPLS label is used as the inner label for VPLS. This label maps to a VPLS routing instance. On the PE router, the LSI label is stripped and then mapped to a logical LSI interface. The Layer 2 Ethernet frame is then forwarded using the LSI interface to the correct VPLS routing instance.

One restriction on flooding behavior in VPLS is that traffic received from remote PE routers is never forwarded to other PE routers. This restriction helps prevent loops in the core network. However, if a CE Ethernet switch has two or more connections to the same PE router, you must enable the Spanning Tree Protocol (STP) on the CE switch to prevent loops. STP is supported on MX Series routers and EX Series switches only.



The Junos OS allows standard Bridge Protocol Data Unit (BPDU) frames to pass through emulated Layer 2 connections, such as those configured with Layer 2 VPNs, Layer 2 circuits, and VPLS routing instances. However, CE Ethernet switches that generate proprietary BPDU frames might not be able to run STP across Juniper Networks routing platforms configured for these emulated Layer 2 connections.



**NOTE:** Under certain circumstances, VPLS provider routers might duplicate an Internet Control Message Protocol (ICMP) reply from a CE router when a PE router has to flood an ICMP request because the destination MAC address has not yet been learned. The duplicate ICMP reply can be triggered when a CE router with promiscuous mode enabled is connected to a PE router. The PE router automatically floods the promiscuous mode-enabled CE router, which then returns the ICMP request to the VPLS provider routers. The VPLS provider routers consider the ICMP request to be new and flood the request again, creating a duplicate ping reply.

## BGP Signaling for VPLS PE Routers Overview

BGP can autonomously signal pseudowires between the PE routers participating in the same virtual private LAN service (VPLS) network. As PE routers are added to and removed from the VPLS network, BGP can signal pseudowires to new PE routers and tear down old pseudowires to old PE routers. Each PE router only needs to be configured with the identity of the VPLS routing instance. Each PE router does not need to be configured with the identities of all of the PE routers that are or might become a part of the VPLS network.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

When you configure BGP for signaling in a VPLS network, customer sites can be either single-homed to a single PE router or multihomed to two or more PE routers. Multihoming provides redundancy for the connection between the customer site and the service provider's network.

You can either configure all of the PE routers in the VPLS network as a full mesh or you can use BGP route reflectors. For full mesh configurations, each PE router needs to be able to create a bidirectional pseudowire to each of the other PE routers participating in the VPLS network.

### Related Documentation

- [VPLS Multihoming Overview on page 705](#)
- [VPLS Path Selection Process for PE Routers on page 175](#)

## Control Word for BGP VPLS Overview

---

In a BGP VPLS network, transit routers must determine the payload for hash calculations for load balancing. While parsing an MPLS encapsulated packet for hashing, a transit router can incorrectly calculate an Ethernet payload as an IPv4 or IPv6 payload if the first nibble of the destination address MAC is 0x4 or 0x6, respectively. This false positive can cause out-of-order packet delivery over a pseudowire. This issue can be avoided by configuring a BGP VPLS edge (VE) router to request that other BGP VE routers insert a control word between the label stack and the MPLS payload.

By inserting a control word between the label stack and the Layer 2 header of a packet traversing a VPLS, the first nibble of the destination address MAC can be ensured to be 0, thus preventing the packet from being identified as an IPv4 or IPv6 packet. All VE routers should want incoming packets to contain control words.

BGP is used to negotiate the support for control words between VE routers. You configure a VE router with the [control-word \(BGP VPLS\)](#) parameter to indicate the preference to receive packets with the control word. By setting the control word, the VE router expects that all frames marked with a label from the VPLS contain the control word. When remote VE routers advertise their NLRI, if the control word is set on them as well, both ends of the pseudowire have control-word support and the control word is expected in packets arriving at the VE routers in both directions.

If a VE router doesn't have the control word set, a VE router that does have a control word set will act as if the VE router without the control word can neither send nor accept BGP VPLS packets with a control word included.

- Related Documentation**
- [Configuring a Control Word for BGP VPLS on page 551](#)
  - [control-word \(BGP VPLS\) on page 1084](#)

## Configuring a Control Word for BGP VPLS

In a BGP VPLS network, transit routers must determine the payload for hash calculations for load balancing. While parsing an MPLS encapsulated packet for hashing, a transit router can incorrectly calculate an Ethernet payload as an IPv4 or IPv6 payload if the first nibble of the destination address MAC is 0x4 or 0x6, respectively. This false positive can cause out-of-order packet delivery over a pseudowire. This issue can be avoided by configuring a BGP VPLS PE router to request that other BGP VPLS edge (VE) routers insert a control word between the label stack and the MPLS payload.



**WARNING:** If you attempt to set a control word in a VPLS network that contains a VE router that does not support a control word, the pseudowire will not come up. To ensure that the pseudowire comes up, be sure that all VE routers in the VPLS network support the presence of a control word.

Before configuring support for a control word in a BGP VPLS network, ensure that the router meets the following requirements:

- MX Series router running Junos OS Release 14.1 or later and containing one of the following Flexible PIC Concentrators: ADPC, NPC, or I-Chip
- OR
- M320 router running Junos OS Release 14.1 or later and containing either the I-Chip or the Trio

To configure a VE router to expect a control word between the label stack and the MPLS payload:

1. At the **[edit routing-instances]** hierarchy level in configuration mode, set **control-word** for the VPLS protocol for the specified routing instance.

```
[edit routing-instances]
user@host# set routing-instance-name protocols vpls control-word
```

For example:

```
[edit routing-instances]
user@host# set vpls1 protocols vpls control-word
```

2. If you are setting **control-word** on a Trio-based MPC on an MX Series router, set **no-ether-pseudowire** to omit the IP payload over the Ethernet pseudowire from the hash key.

```
[edit forwarding-options]
user@host# set enhanced-hash-key family mpls no-ether-pseudowire
```

3. Verify the configuration.

```
[edit routing-instances]
user@host# show
vpls1 {
 protocols {
 vpls {
```

```

 control-word;
 }
}

[edit forwarding-options]
user@host# show
enhanced-hash-key {
 family mpls {
 no-ether-pseudowire;
 }
}

```

4. Repeat the configuration on each VE router in the BGP VPLS network.
5. Run **show vpls connections instance *routing-instance-name* extensive** to verify the presence of a control word for the pseudowire.

For example:

```

user@host# show vpls connections instance vpls1 extensive
Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid NC -- interface encapsulation not CCC/TCC/VPLS
...
PF -- Profile parse failure PB -- Profile busy

Legend for interface status
Up -- operational
Dn -- down

Instance: vpls1
...
 connection-site Type St Time last up # Up trans
 1 rmt Up May 21 10:08:34 2013 2
 Remote PE: 192.0.2.1, Negotiated control-word: Yes

```

- Related Documentation**
- [Control Word for BGP VPLS Overview on page 550](#)
  - [control-word \(BGP VPLS\) on page 1084](#)
  - [no-control-word \(BGP VPLS\) on page 1164](#)

## BGP Route Reflectors for VPLS

In large networks, it might be necessary to configure BGP route reflectors to reduce the control plane workload for the routers participating in the VPLS network. BGP route reflectors can help to reduce the workload of the network control plane in the following ways.

- Making it unnecessary to configure all of the VPLS PE routers in a full mesh.
- Limiting the total volume of BGP VPLS messages exchanged within the network by transmitting messages to interested routers only (instead of all of the BGP routers in the network)

- Reducing the network signaling load whenever another BGP router is added to or removed from the network

The basic solution to these problems is to deploy a small group of BGP route reflectors that are in a full mesh with one another. Each of the VPLS PE routers is configured to have a BGP session with one or more of the route reflectors, making it unnecessary to maintain a full mesh of BGP sessions between all of the PE routers.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

This type of configuration only affects the control plane of the VPLS network (how routers signal and tear down pseudowires to one another in the network). The actual data plane state and forwarding paths for the VPLS traffic are not modified by the route reflectors. Effectively, the VPLS pseudowires should take the same paths across the network whether or not you have configured route reflectors. For a description of how VPLS selects the best path to a PE router, see “[VPLS Path Selection Process for PE Routers](#)” on page 175.

The MAC addresses themselves are not exchanged or processed in any way by BGP. Each VPLS PE router performs all MAC address learning and aging individually. BGP's only function relative to VPLS is to exchange messages related to automatic discovery of PE routers being added to and removed from the VPLS network and the MPLS label exchange needed to signal a pseudowire from one PE router to another.

#### Related Documentation

- [VPLS Path Selection Process for PE Routers on page 175](#)
- [Example: Configuring a Route Reflector](#)
- [Example: NG-VPLS Using Point-to-Multipoint LSPs on page 815](#)
- [Example: Next-Generation VPLS for Multicast with Multihoming on page 787](#)

## Interoperability Between BGP Signaling and LDP Signaling in VPLS

You can configure a VPLS routing instance where some of the PE routers use BGP for signaling and some use LDP for signaling.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

The following concepts form the basis of the configuration needed to include both BGP-signaled and LDP-signaled PE routers in a VPLS routing instance:

- **PE router mesh group**—Consists of a set of routers participating in a VPLS routing instance that share the same signaling protocol, either BGP or LDP, and are also fully meshed. Each VPLS routing instance can have just one BGP mesh group. However, you can configure multiple LDP mesh groups for each routing instance.
- **Border router**—A PE router that must be reachable by all of the other PE routers participating in a VPLS routing instance, whether they are LDP-signaled or BGP-signaled. Bidirectional pseudowires are created between the border router and all of these PE routers. The border router is aware of the composition of each PE mesh group configured as a part of the VPLS routing instance. It can also have direct connections to local CE routers, allowing it to act as a typical PE router in a VPLS routing instance.

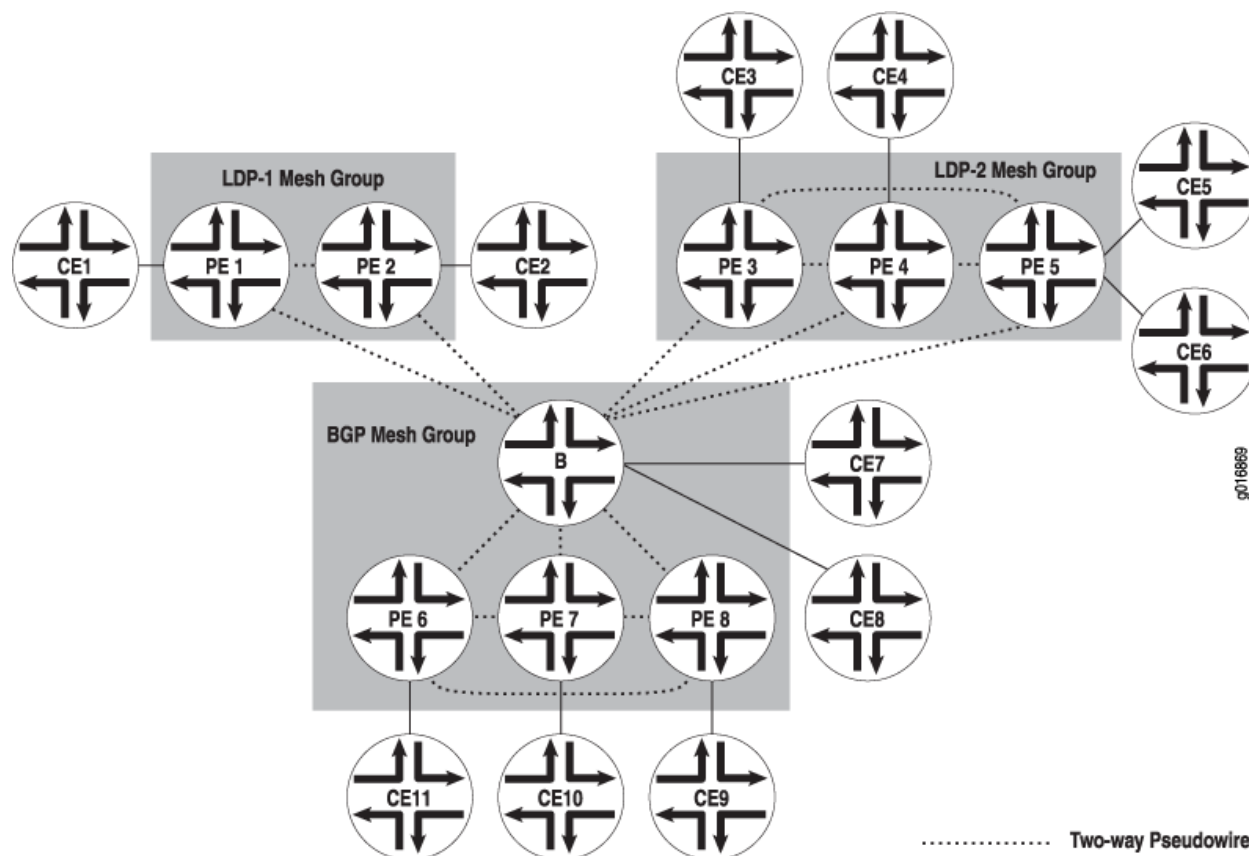
The following sections describe how the LDP-signaled and BGP-signaled PE routers function when configured to interoperate within a VPLS routing instance:

- [LDP-Signaled and BGP-Signaled PE Router Topology on page 554](#)
- [Flooding Unknown Packets Across Mesh Groups on page 556](#)
- [Unicast Packet Forwarding on page 556](#)

### LDP-Signaled and BGP-Signaled PE Router Topology

[Figure 49 on page 555](#) illustrates a topology for a VPLS routing instance configured to support both BGP and LDP signaling. Router B is the border router. Routers PE1 and PE2 are in the LDP-signaled mesh group LDP-1. Routers PE3, PE4, and PE5 are in the LDP-signaled mesh group LDP-2. Routers PE6, PE7, PE8, and router B (the border router) are in the BGP-signaled mesh group. The border router also acts as a standard VPLS PE router (having local connections to CE routers). All of the PE routers shown are within the same VPLS routing instance.

Figure 49: BGP and LDP Signaling for a VPLS Routing Instance



Two-way pseudowires are established between the PE routers in each mesh group and between each PE router in the VPLS routing instance and the border router. In [Figure 49 on page 555](#), two-way pseudowires are established between routers PE1 and PE2 in mesh group LDP-1, routers PE3, PE4, and PE5 in mesh group LDP-2, and routers PE6, PE7, and PE8 in the BGP mesh group. Routers PE1 through PE8 also all have two-way pseudowires to the Border router. Based on this topology, the LDP-signaled routers are able to interoperate with the BGP-signaled routers. Both the LDP-signaled and BGP-signaled PE routers can logically function within a single VPLS routing instance.



**NOTE:** The following features are not supported for VPLS routing instances configured with both BGP and LDP signaling:

- Point-to-multipoint LSPs
- Integrated routing and bridging
- IGMP snooping

## Flooding Unknown Packets Across Mesh Groups

Broadcast, multicast, and unicast packets of unknown origin received from a PE router are flooded to all local CE routers. They are also flooded to all of the PE routers in the VPLS routing instance except the PE routers that are a part of the originating PE router mesh group.

For example, if a multicast packet is received by the border router in [Figure 49 on page 555](#), it is flooded to the two local CE routers. It is also flooded to routers PE1 and PE2 in the LDP-1 mesh group and to routers PE3, PE4, and PE5 in the LDP-2 mesh group. However, the packet is not flooded to routers PE6, PE7, and PE8 in the BGP mesh group.

## Unicast Packet Forwarding

The PE border router is made aware of the composition of each PE router mesh group. From the data plane, each PE router mesh group is viewed as a virtual pseudowire LAN. The border router is configured to interconnect all of the PE router mesh groups belonging to a single VPLS routing instance. To interconnect the mesh groups, a common MAC table is created on the border router.

Unicast packets originating within a mesh group are dropped if the destination is another PE router within the same mesh group. However, if the destination MAC address of the unicast packet is a PE router located in a different mesh group, the packet is forwarded to that PE router.

## Configuring Interoperability Between BGP Signaling and LDP Signaling in VPLS

---

A single VPLS routing instance can encompass one set of PE routers that use BGP for signaling and another set of PE routers that use LDP for signaling. Within each set, all of the PE routers are fully meshed in both the control and data planes and have a bidirectional pseudowire to each of the other routers in the set. However, the BGP-signaled routers cannot be directly connected to the LDP-signaled routers. To be able to manage the two separate sets of PE routers in a single VPLS routing instance, a border PE router must be configured to interconnect the two sets of routers.

The VPLS RFCs and Internet drafts require that all of the PE routers participating in a single VPLS routing instance must be fully meshed in the data plane. In the control plane, each fully meshed set of PE routers in a VPLS routing instance is called a PE router mesh group. The border PE router must be reachable by and have bidirectional pseudowires to all of the PE routers that are a part of the VPLS routing instance, both the LDP-signaled and BGP-signaled routers.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

---

For LDP BGP interworking to function, LDP-signaled routers can be configured with forwarding equivalence class (FEC) 128 or FEC 129.



The following sections describe how to configure BGP LDP interworking for VPLS:

- [LDP BGP Interworking Platform Support on page 557](#)
- [Configuring FEC 128 VPLS Mesh Groups for LDP BGP Interworking on page 557](#)
- [Configuring FEC 129 VPLS Mesh Groups for LDP BGP Interworking on page 558](#)
- [Configuring Switching Between Pseudowires Using VPLS Mesh Groups on page 558](#)
- [Configuring Integrated Routing and Bridging Support for LDP BGP Interworking with VPLS on page 559](#)
- [Configuring Inter-AS VPLS with MAC Processing at the ASBR on page 559](#)

## LDP BGP Interworking Platform Support

LDP BGP interworking is supported on the following Juniper Networks routers and routing platforms:

- M7i
- M10i
- M40e
- M120
- M320
- MX Series routers
- T Series routers
- TX Matrix routers
- EX Series switches

## Configuring FEC 128 VPLS Mesh Groups for LDP BGP Interworking

To configure FEC 128 LDP BGP interworking for VPLS, include the **mesh-group** statement in the VPLS routing instance configuration of the PE border router:

```
mesh-group mesh-group-name {
 local-switching;
 mac-flush [explicit-mac-flush-message-options];
 neighbor address;
 peer-as all;
 vpls-id number;
}
```

You can include this statement at the following hierarchy levels:

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

Using the **neighbor** statement, configure each PE router that is a part of the mesh group. You must separate the LDP-signaled routers and the BGP-signaled routers into their own

respective mesh groups. The LDP-signaled routers can be divided into multiple mesh groups. The BGP-signaled routers must be configured within a single mesh group for each routing instance.

## Configuring FEC 129 VPLS Mesh Groups for LDP BGP Interworking

Configuration for a mesh group for FEC 129 is very similar to the configuration for FEC 128.

Note the following differences for FEC 129:

- Each user-defined mesh group must have a unique route distinguisher. Do not use the route distinguisher that is defined for the default mesh group at the **[edit routing-instances]** hierarchy level.
- Each user-defined mesh group must have its own import and export route target.
- Each user-defined mesh group can have a unique Layer 2 VPN ID. By default, all the mesh groups that are configured for the a VPLS routing-instance use the same Layer 2 VPN ID, the one that you configure at the **[edit routing-instances]** hierarchy level.

## Configuring Switching Between Pseudowires Using VPLS Mesh Groups

To configure switching between Layer 2 circuit pseudowires using VPLS mesh groups, you can do either of the following:

- Configure a mesh group for each Layer 2 circuit pseudowire terminating at a VPLS routing instance. The Junos OS can support up to 16 mesh groups on MX Series routers and up to 128 on M Series and T Series routers. However, two mesh groups are created by default, one for the CE routers and one for the PE routers. Therefore, the maximum number of user-defined mesh groups is 14 for MX Series routers and 126 for M Series and T Series routers.
- Configure a single mesh group, terminate all the Layer 2 circuit pseudowires into it, and enable local switching between the pseudowires by including the **local-switching** statement at the **[edit routing-instances routing-instance-name protocols vpls mesh-group mesh-group-name]** hierarchy level. By default, you cannot configure local switching for mesh groups (except for the CE mesh group) because all of the VPLS PE routers must be configured in a full mesh. However, local switching is useful if you are terminating Layer 2 circuit pseudowires in a mesh group configured for an LDP signaled VPLS routing instance.



**NOTE:** Do not include the **local-switching** statement on PE routers configured in a full mesh VPLS network.

---

To terminate multiple pseudowires at a single VPLS mesh group, include the **local-switching** statement:

**local-switching;**

You can include this statement at the following hierarchy levels:

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

## Configuring Integrated Routing and Bridging Support for LDP BGP Interworking with VPLS

Beginning with Junos OS Release 9.4, you can configure an integrated routing and bridging (IRB) interface on a router that functions as an autonomous system border router (ASBR) in an inter-AS VPLS environment between BGP-signaled VPLS and LDP-signaled VPLS. Previously, IRB interfaces were supported only on Provider Edge (PE) routers.

To configure a IRB support for LDP BGP Interworking with VPLS, include the **routing-interface *interface-name*** statement.

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name*]
- [edit logical-routers *logical-router-name* routing-instances *routing-instance-name*]

## Configuring Inter-AS VPLS with MAC Processing at the ASBR

Inter-AS VPLS with MAC processing at the ASBR enables you to interconnect customer sites that are located in different ASs. In addition, you can configure the ASs with different signaling protocols. You can configure one of the ASs with BGP-signaled VPLS and the other with LDP-signaled VPLS. For more information about how to configure LDP-signaled and BGP signaled VPLS, see [“Configuring Interoperability Between BGP Signaling and LDP Signaling in VPLS” on page 556](#).

For inter-AS VPLS to function properly, you need to configure IBGP peering between the PE routers, including the ASBRs in each AS, just as you do for a typical VPLS configuration. You also need to configure EBGP peering between the ASBRs in the separate ASs. The EBGP peering is needed between the ASBRs only. The link between the ASBR routers does not have to be Ethernet. You can also connect a CE router directly to one of the ASBRs, meaning you do not have to have a PE router between the ASBR and the CE router.

The configuration for the connection between the ASBRs makes inter-AS VPLS with MAC operations unique. The other elements of the configuration are described in other sections of this manual. An extensive configuration example for inter-AS VPLS with MAC operations is provided in the *Junos OS, Release 15.1*.

The following sections describe how to configure inter-AS VPLS with MAC operations:

- [Inter-AS VPLS with MAC Operations Configuration Summary on page 560](#)
- [Configuring the ASBRs for Inter-AS VPLS on page 560](#)

### Inter-AS VPLS with MAC Operations Configuration Summary

---

This section provides a summary of all of the elements which must be configured to enable inter-AS VPLS with MAC operations. These procedures are described in detail later in this chapter and in other parts of the *Junos OS VPNs Library for Routing Devices*.

The following lists all of major elements of an inter-AS VPLS with MAC operations configuration:

- Configure IBGP between all of the routers within each AS, including the ASBRs.
- Configure EBGP between the ASBRs in the separated ASs. The EBGP configuration includes the configuration that interconnects the ASs.
- Configure a full mesh of LSPs between the ASBRs.
- Configure a VPLS routing instance encompassing the ASBR routers. The ASBRs are VPLS peers and are linked by a single pseudowire. Multihoming between ASs is not supported. A full mesh of pseudowires is needed between the ASBR routers in all of the interconnected ASs.
- Configure the VPLS routing instances using either BGP signaling or LDP signaling. LDP BGP interworking is supported for inter-AS VPLS with MAC operations, so it is possible to interconnect the BGP-signaled VPLS routing instances with the LDP-signaled VPLS routing instances.
- Configure a single VPLS mesh group for all of the ASBRs interconnected using inter-AS VPLS.

### Configuring the ASBRs for Inter-AS VPLS

---

This section describes the configuration on the ASBRs needed to enable inter-AS VPLS with MAC operations.

On each ASBR, you need to configure a VPLS mesh group within the VPLS routing instance which needs to include all of the PE routers within the AS, in addition to the ASBR. You need to configure the same mesh group for each of the ASs you want to interconnect using inter-AS VPLS. The mesh group name should be identical on each AS. You also must include the **peer-as all** statement. This statement enables the router to establish a single pseudowire to each of the other ASBRs.

To configure the mesh group on each ASBR, include the **mesh-group** and **peer-as all** statements:

```
mesh-group mesh-group-name {
 peer-as all;
}
```

You can include these statements at the following hierarchy levels:

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

- Related Documentation**
- [Example: Configuring BGP Autodiscovery for LDP VPLS on page 725](#)
  - [Example: Configuring BGP Autodiscovery for LDP VPLS with User-Defined Mesh Groups on page 742](#)



# Assigning Routing Instances to VPLS

- [Configuring VPLS Routing Instances on page 563](#)
- [PE Router Mesh Groups for VPLS Routing Instances on page 576](#)
- [Configuring VPLS Fast Reroute Priority on page 577](#)
- [Specifying the VT Interfaces Used by VPLS Routing Instances on page 579](#)
- [Understanding PIM Snooping for VPLS on page 579](#)
- [Example: Configuring PIM Snooping for VPLS on page 581](#)
- [VPLS Label Blocks Operation on page 591](#)
- [Configuring the Label Block Size for VPLS on page 596](#)
- [Example: Building a VPLS From Router 1 to Router 3 to Validate Label Blocks on page 596](#)

## Configuring VPLS Routing Instances

---

To configure a VPLS routing instance, include the **vpls** statement:

```
vpls {
 active-interface {
 any;
 primary interface-name;
 }
 connectivity-type (ce | irb | permanent);
 control-word;
 encapsulation-type encapsulation-type;
 interface-mac-limit limit;
 label-block-size size;
 mac-table-aging-time time;
 mac-table-size size;
 neighbor neighbor-id;
 no-control-word;
 no-tunnel-services;
 site site-name {
 active-interface {
 any;
 primary interface-name;
 }
 interface interface-name {
 interface-mac-limit limit;
 }
 }
}
```

```

 mesh-group mesh-group-name;
 multi-homing;
 site-identifier identifier;
 site-preference preference-value {
 backup;
 primary;
 }
}
site-range number;
traceoptions {
 file filename <files number> <size size> <world-readable | no-world-readable>;
 flag flag <flag-modifier> <disable>;
}
tunnel-services {
 devices device-names;
 primary primary-device-name;
}
vpls-id vpls-id;
}

```

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]



**NOTE:** You cannot configure a routing protocol (OSPF, RIP, IS-IS or BGP) inside a VPLS routing instance (*instance-type vpls*). The Junos CLI disallows this configuration.

The configuration for the VPLS routing instance statements is explained in the following sections:

- [Configuring BGP Signaling for VPLS on page 564](#)
- [Configuring LDP Signaling for VPLS on page 569](#)
- [Configuring VPLS Routing Instance and VPLS Interface Connectivity on page 572](#)
- [Configuring the VPLS Encapsulation Type on page 573](#)
- [Configuring the VPLS MAC Table Timeout Interval on page 573](#)
- [Configuring the Size of the VPLS MAC Address Table on page 574](#)
- [Limiting the Number of MAC Addresses Learned from an Interface on page 574](#)
- [Removing Addresses from the MAC Address Database on page 576](#)

## Configuring BGP Signaling for VPLS

You can configure BGP signaling for the VPLS routing instance. BGP is used to signal the pseudowires linking each of the PE routers participating in the VPLS routing instance. The pseudowires carry VPLS traffic across the service provider's network between the VPLS sites.





**NOTE:** You cannot configure both BGP signaling and LDP signaling for the same VPLS routing instance. If you attempt to configure the statements that enable BGP signaling for the VPLS routing instance (the `site`, `site-identifier`, and `site-range` statements) and the statements that enable LDP signaling for the same instance (the `neighbor` and `vpls-id` statements), the commit operation fails.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

Configure BGP signaling for the VPLS routing instance by completing the steps in the following sections:

- [Configuring the VPLS Site Name and Site Identifier on page 565](#)
- [Configuring Automatic Site Identifiers for VPLS on page 566](#)
- [Configuring the Site Range on page 566](#)
- [Configuring the VPLS Site Interfaces on page 568](#)
- [Configuring the VPLS Site Preference on page 569](#)

### Configuring the VPLS Site Name and Site Identifier

When you configure BGP signaling for the VPLS routing instance, on each PE router you must configure each VPLS site that has a connection to the PE router. All the Layer 2 circuits provisioned for a VPLS site are listed as the set of logical interfaces (using the `interface` statement) within the `site` statement.

You must configure a site name and site identifier for each VPLS site.

To configure the site name and the site identifier, include the `site` and the `site-identifier` statements:

```
site site-name {
 interface interface-name {
 interface-mac-limit limit;
 }
 site-identifier identifier;
}
```

The numerical identifier can be any number from 1 through 65,534 that uniquely identifies the local VPLS site.

You can include these statements at the following hierarchy levels:

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

### Configuring Automatic Site Identifiers for VPLS

---

When you enable automatic site identifiers, the Junos OS automatically assigns site identifiers to VPLS sites. To configure automatic site identifiers for a VPLS routing instance, include the **automatic-site-id** statement:

```
automatic-site-id {
 collision-detect-time seconds;
 new-site-wait-time seconds;
 reclaim-wait-time minimum seconds maximum seconds;
 startup-wait-time seconds;
}
```

You can include this statement at the following hierarchy levels:

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

The **automatic-site-id** statement includes a number of options that control different delays in network layer reachability information (NLRI) advertisements. All of these options are configured with default values. See the statement summary for the **automatic-site-id** statement for more information.

The **automatic-site-id** statement includes the following options:

- **collision-detect-time**—The time in seconds to wait after a claim advertisement is sent to the other routers in a VPLS instance before a PE router can begin using a site identifier. If the PE router receives a competing claim advertisement for the same site identifier during this time period, it initiates the collision resolution procedure for site identifiers.
- **new-site-wait-time**—The time in seconds to wait to receive VPLS information for a newly configured routing instance or a new site. This time interval is also applied whenever the automatic site identifier feature is activated on a VPLS routing instance other than at startup. Effectively, this timer indicates how long to wait before an attempt is made to allocate a site identifier. This timer is also triggered whenever a VPLS routing instance is enabled.
- **reclaim-wait-time**—The time to wait before attempting to claim a site identifier after a collision. A collision occurs whenever an attempt is made to claim a site identifier by two separate VPLS sites.
- **startup-wait-time**—The time in seconds to wait at startup to receive all the VPLS information for the route targets configured on the other PE routers included in the VPLS routing instance.

### Configuring the Site Range

---

When you enable BGP signaling for each VPLS routing instance, you can optionally configure the site range. The site range specifies an upper limit on the maximum site identifier that can be accepted to allow a pseudowire to be brought up. You must specify a value from 1 through 65,534. The default value is 65,534. We recommend using the

default. Pseudowires cannot be established to sites with site identifiers greater than the configured site range. If you issue the **show vpls connections** command, such sites are displayed as OR (out of range).

To configure the site range, include the **site-range** statement:

```
site-range number;
```

You can include this statement at the following hierarchy levels:

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

There are networks that require that the site range be configured using a value smaller than the local site identifier, for example, a hub-and-spoke VPLS with multihomed sites. For this type of network, you need to allow pseudowires to be established between the spoke routers and the hub router. However, you also need to prevent pseudowires from being established between spoke routers directly. Due to the multihoming requirement of spoke sites, Layer 2 VPN NRLIs need to be accepted from other spoke routers (at least from spokes with the same site identifier as the locally configured sites) to determine the status of local spoke routers (active or not active) based on the local preference included in the NRLIs received from the other spoke routers.

This type of VPLS network can be implemented by, for example, numbering hub sites with identifiers 1 through 8 and spoke sites with identifiers 9 and larger. You can then configure a site range of 8 on each of the spoke sites. Although the spoke sites accept NRLIs and install them in the Layer 2 VPN routing tables (allowing the multihomed sites to determine the status of the local site), the spoke sites cannot establish pseudowires directly to the other spoke sites due to the configured site range.

The following configurations illustrate this concept. The configurations are for the VPLS routing instances on three routers, two spoke routers and one hub router:

Router 1—spoke:

```
routing-instance hub-and-spoke {
 no-local-switching;
 protocols {
 vpls {
 site-range 8;
 no-tunnel-services;
 site spoke-9 {
 site-identifier 9 {
 multi-homing;
 site-preference primary;
 }
 }
 site spoke-10 {
 site-identifier 10 {
 multi-homing;
 site-preference backup;
 }
 }
 }
 }
}
```

```

 }
 }
}

```

Router 2—spoke:

```

routing-instance hub-and-spoke {
 no-local-switching;
 protocols {
 vpls {
 site-range 8;
 no-tunnel-services;
 site spoke-9 {
 site-identifier 9 {
 multi-homing;
 site-preference backup;
 }
 }
 site spoke-10 {
 site-identifier 10 {
 multi-homing;
 site-preference primary;
 }
 }
 }
 }
}

```

Hub—router 3:

```

routing-instance hub-and-spoke {
 no-local-switching;
 protocols {
 vpls {
 no-tunnel-services;
 site hub {
 site-identifier 1;
 }
 }
 }
}

```

### Configuring the VPLS Site Interfaces

You must configure an interface for each of the pseudowires you specify for the VPLS site.

To configure an interface for the VPLS site, include the **interface** statement:

```

interface interface-name {
 interface-mac-limit limit;
}

```

You can include these statements at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols vpls site *site-name*]

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

You can also configure a limit on the number of MAC addresses that can be learned from the specified interface. For more information, see [“Limiting the Number of MAC Addresses Learned from an Interface” on page 574](#).

### Configuring the VPLS Site Preference

You can specify the local preference value advertised for a particular VPLS site. The site preference value is specified using the **site-preference** statement configured at the `[edit routing-instances routing-instance-name protocols vpls site site-name]` hierarchy level. By configuring the **site-preference** statement, a value configured for the **local-preference** statement at the `[edit protocols bgp]` hierarchy level is ignored by the VPLS routing instance. However, you can change the site preference value for VPLS routes exported to other routers by configuring an export policy. When a PE router receives multiple advertisements with the same VPLS edge (VE) device identifier, the advertisement with the highest local preference value is preferred.

To configure the VPLS site preference, include the **site-preference** statement:

```
site-preference preference-value {
 backup;
 primary;
}
```

You can also specify either the **backup** option or the **primary** option for the **site-preference** statement. The **backup** option specifies the preference value as 1, the lowest possible value, ensuring that the VPLS site is the least likely to be selected. The **primary** option specifies the preference value as 65,535, the highest possible value, ensuring that the VPLS site is the most likely to be selected.

For a list of hierarchy levels at which you can include the **site-preference** statement, see the statement summary section for this statement.

### Configuring LDP Signaling for VPLS

You can configure LDP as the signaling protocol for a VPLS routing instance. This functionality is described in RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*.

The Junos OS software does not support all of RFC 4762. When enabling LDP signaling for a VPLS routing instance, network engineers should be aware that only the following values are supported:

- FEC—128 or 129
- Control bit—0
- Ethernet pseudowire type—0x0005
- Ethernet tagged mode pseudowire type—0x0004

LDP signaled VPLS supports the Virtual Circuit Connectivity Verification (VCCV) Type Length Value (TLV) for pseudowire label mapping, label database display, and LDP trace. When you enable LDP signaling for a pseudowire, LDP advertises the VCCV capabilities to the neighboring routers. VCCV provides a control channel for a pseudowire and includes both operations and management functions (for example, connectivity verification). This control channel is established between the pseudowire's ingress and egress devices. Once established, connectivity verification messages can be sent over the VCCV control channel.

The Junos OS software supports the following VCCV capabilities for LDP signaled VPLS (defined in RFC 5085 Section 8.1):

- VCCV connectivity check types:
  - Router Alert Label
  - MPLS pseudowire label with TTL=1
- VCCV connectivity verification type:
  - LSP ping

If the peer device also advertises VCCV parameters during pseudowire setup, the Junos OS software selects the set of common advertised parameters to use as the method for performing VCCV OAM on the pseudowire.

The locally advertised and peer advertised VCCV parameters can be viewed using the **show ldp database** command as show here:

```
user@host> show ldp database l2circuit extensive
Input label database, 10.255.245.198:0--10.255.245.194:0
 Label Prefix
 299872 L2CKT CtrlWord PPP VC 100
 MTU: 4470
 VCCV Control Channel types:
 MPLS router alert label
 MPLS PW label with TTL=1
 VCCV Control Verification types:
 LSP ping
 Label Prefix
 State: Active
 Age: 19:23:08
```

Be aware of the following behavior with regard to TLVs when configuring LDP-signaled VPLS in a network with equipment from other vendors:

- When a Juniper Network's device receives a TLV with an empty address, LDP accepts the TLV.
- When a MAC address is withdrawn, LDP specifies a zero address (0.0.0.0) for the AddressList.

To enable LDP signaling for the set of PE routers participating in the same VPLS routing instance, you need to use the **vpls-id** statement configured at the **[edit routing-instances routing-instance-name protocols vpls]** hierarchy level to configure the same VPLS identifier on each of the PE routers. The VPLS identifier must be globally unique. When each VPLS

routing instance (domain) has a unique VPLS identifier, it is possible to configure multiple VPLS routing instances between a given pair of PE routers.

LDP signaling requires that you configure a full-mesh LDP session between the PE routers in the same VPLS routing instance. Neighboring PE routers are statically configured. Tunnels are created between the neighboring PE routers to aggregate traffic from one PE router to another. Pseudowires are then signaled to demultiplex traffic between VPLS routing instances. These PE routers exchange the pseudowire label, the MPLS label that acts as the VPLS pseudowire demultiplexer field, by using LDP forwarding equivalence classes (FECs). Tunnels based on both MPLS and generic routing encapsulation (GRE) are supported.



**NOTE:** You cannot configure both BGP signaling and LDP signaling for the same VPLS routing instance. If you attempt to configure the statements that enable BGP signaling for the VPLS routing instance (the `site`, `site-identifier`, and `site-range` statements), and the statements that enable LDP signaling for the same instance, `neighbor` and `vpls-id`, the commit operation fails.

To enable LDP signaling for the VPLS routing instance, complete the steps in the following sections:

- [Configuring LDP Signaling for the VPLS Routing Instance on page 571](#)
- [Configuring LDP Signaling on the Router on page 572](#)

### Configuring LDP Signaling for the VPLS Routing Instance

To configure the VPLS routing instance to use LDP signaling, you must configure the same VPLS identifier on each PE router participating in the instance. Specify the VPLS identifier with the `vpls-id` statement:

```
vpls-id vpls-id;
```

You can include this statement at the following hierarchy levels:

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

To configure the VPLS routing instance to use LDP signaling, you also must include the `neighbor` statement to specify each of the neighboring PE routers that are a part of this VPLS domain:

```
neighbor neighbor-id;
```

You can include this statement at the following hierarchy levels:

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

### Configuring LDP Signaling on the Router

---

To enable LDP signaling, you need to configure LDP on each PE router participating in the VPLS routing instance. A minimal configuration is to enable LDP on the loopback interface, which includes the router identifier (**router-id**), on the PE router using the **interface** statement:

```
interface interface-name;
```

You can include this statement at the following hierarchy levels:

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

You can enable LDP on all the interfaces on the router using the **all** option for the **interfaces** statement. For more information about how to configure LDP, see the *Junos OS MPLS Applications Library for Routing Devices*.

### Configuring VPLS Routing Instance and VPLS Interface Connectivity

You can configure the VPLS routing instance to take down or maintain its VPLS connections depending on the status of the interfaces configured for the VPLS routing instance. By default, the VPLS connection is taken down whenever a customer-facing interface configured for the VPLS routing instance fails. This behavior can be explicitly configured by specifying the **ce** option for the **connectivity-type** statement:

```
connectivity-type ce;
```

You can alternatively specify that the VPLS connection remain up so long as an Integrated Routing and Bridging (IRB) interface is configured for the VPLS routing instance by specifying the **irb** option for the **connectivity-type** statement:

```
connectivity-type irb;
```

To ensure that the VPLS connection remain up until explicitly taken down, specify the **permanent** option for the **connectivity-type** statement:

```
connectivity-type permanent;
```

This option is reserved for use in configuring Layer 2 Wholesale subscriber networks. See the *Broadband Subscriber Management Solutions Guide* for details about configuring a Layer 2 Wholesale network.

You can include this statement at the following hierarchy levels:

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



## Configuring the VPLS Encapsulation Type

You can specify a VPLS encapsulation type for the pseudowires established between VPLS neighbors. The encapsulation type is carried in the LDP-signaling messages exchanged between VPLS neighbors when pseudowires are created. You might need to alter the encapsulation type depending on what other vendors' equipment is deployed within your network.

VPLS effectively provides a bridge between Ethernet networks. As a consequence, only two encapsulation types are available:

- **ethernet**—Ethernet
- **ethernet-vlan**—Ethernet virtual LAN (VLAN)

If you do not specify an encapsulation type for the VPLS routing instance or the VPLS neighbor, **ethernet** is used.

To specify an encapsulation type for the VPLS routing instance, include the **encapsulation-type** statement:

```
encapsulation-type (ethernet | ethernet-vlan);
```

You can include this statement at the following hierarchy levels:

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

You can also specify an encapsulation type for a specific VPLS neighbor by including the **encapsulation-type** statement at the following hierarchy levels:

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

## Configuring the VPLS MAC Table Timeout Interval

You can modify the timeout interval for the VPLS table. We recommend you that configure longer values for small, stable VPLS networks and shorter values for large, dynamic VPLS networks. If the VPLS table does not receive any updates during the timeout interval, the router waits one additional interval before automatically clearing the MAC address entries from the VPLS table.

To modify the timeout interval for the VPLS table, include the **mac-table-aging-time** statement:

```
mac-table-aging-time seconds;
```

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols vpls]

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



**NOTE:** The `mac-table-aging-time` statement is not available on MX Series routers.

---

## Configuring the Size of the VPLS MAC Address Table

You can modify the size of the VPLS media access control (MAC) address table. The default table size is 512 MAC addresses, the minimum is 16 addresses, and the maximum is 65,536 addresses.



**NOTE:** T4000 routers with Type 5 FPCs support up to 262,143 MAC addresses per VPLS routing instance. To enable the improved VPLS MAC address learning limit (that is, 262,143 MAC addresses), you must include the `enhanced-mode` statement at the [edit chassis network-services] hierarchy level, reboot the router, and then modify the size of the VPLS MAC address table.

If the MAC table limit is reached, new MAC addresses can no longer be added to the table. Eventually the oldest MAC addresses are removed from the MAC address table automatically. This frees space in the table, allowing new entries to be added. However, as long as the table is full, new MAC addresses are dropped.

To change the VPLS MAC table size for each VPLS or VPN routing instance, include the `mac-table-size` statement:

```
mac-table-size size;
```

You can include this statement at the following hierarchy levels:

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

When you include the `mac-table-size` statement, the affected interfaces include all interfaces within the VPLS routing instance, including the local interfaces, the LSI interfaces, and the VT interfaces.

## Limiting the Number of MAC Addresses Learned from an Interface

You can configure a limit on the number of MAC addresses learned by a VPLS routing instance using the `mac-table-size` statement. If the MAC table limit is reached, new MAC addresses can no longer be added to the table. Eventually the oldest MAC addresses are removed from the MAC address table automatically. This frees space in the table, allowing new entries to be added. However, as long as the table is full, new MAC addresses are dropped.

Because this limit applies to each VPLS routing instance, the MAC addresses of a single interface can consume all the available space in the table, preventing the routing instance from acquiring addresses from other interfaces.

You can limit the number of MAC addresses learned from each interface configured for a VPLS routing instance. To do so, include the **interface-mac-limit** statement:

```
interface-mac-limit limit;
```

You can include this statement at the following hierarchy levels:

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

The **interface-mac-limit** statement affects the local interfaces only (the interfaces facing CE devices).

Configuring the **interface-mac-limit** statement at the [edit routing-instances *routing-instance-name* protocols vpls] hierarchy level causes the same limit to be applied to all of the interfaces configured for that specific routing instance.



**NOTE:** Starting with Junos OS Release 12.3R4, if you do not configure the parameter to limit the number of MAC addresses to be learned by a VPLS instance, the default value is not effective. Instead, if you do not include the **interface-mac-limit** option at the [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vpls site *site-name* interfaces *interface-name*], hierarchy level, this setting is not present in the configuration with the default value of 1024 addresses. If you upgrade a router running a Junos OS release earlier than Release 12.3R4 to Release 12.3R4 or later, you must configure the **interface-mac-limit** option with a valid value for it to be saved in the configuration.

You can also limit the number of MAC addresses learned by a specific interface configured for a VPLS routing instance. This gives you the ability to limit particular interfaces that you expect might generate a lot of MAC addresses.

To limit the number of MAC addresses learned by a specific interface, include the **interface-mac-limit** statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols vpls site *site-name* interfaces *interface-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vpls site *site-name* interfaces *interface-name*]

The MAC limit configured for an individual interface at this hierarchy level overrides any value configured at the [edit routing-instances *routing-instance-name* protocols vpls] hierarchy level. Also, the MAC limit configured using the **mac-table-size** statement can override the limit configured using the **interface-mac-limit** statement.

The MAC address limit applies to customer-facing interfaces only.

## Removing Addresses from the MAC Address Database

You can enable MAC flush processing for the VPLS routing instance or for the mesh group under a VPLS routing instance. MAC flush processing removes MAC addresses from the MAC address database that have been learned dynamically. With the dynamically learned MAC addresses removed, MAC address convergence requires less time to complete.

You can clear dynamically learned MAC addresses from the MAC address database by including the **mac-flush** statement:

**mac-flush** [ *explicit-mac-flush-message-options* ];

To clear dynamically learned MAC addresses globally across all devices participating in the routing instance, you can include the statement at the following hierarchy levels:

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

To clear the MAC addresses on the routers in a specific mesh group, you can include the statement at the following hierarchy levels:

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

For certain cases where MAC flush processing is not initiated by default, you can also specify **explicit-mac-flush-message-options** to additionally configure the router to send explicit MAC flush messages under specific conditions. For a list of the explicit MAC flush message options you can include with this statement, see the summary section for this statement.

### Related Documentation

- [Configuring Improved VPLS MAC Address Learning on T4000 Routers with Type 5 FPCs on page 918](#)
- *enhanced-mode*
- *show ldp database*

---

## PE Router Mesh Groups for VPLS Routing Instances

A PE router mesh group consists of a set of routers participating in a VPLS routing instance that share the same signaling protocol, either BGP or LDP. Each VPLS routing instance can have just one BGP mesh group. However, you can configure multiple LDP mesh groups for each routing instance.

The Junos OS can support up to 16 mesh groups on MX Series routers and up to 128 on M Series and T Series routers. However, two mesh groups are created by default, one for

the CE routers and one for the PE routers. Therefore, the maximum number of user-defined mesh groups is 14 for MX Series routers and 126 for M Series and T Series routers.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

The Junos OS supports both forwarding equivalency class (FEC) 128 and FEC 129. FEC 129 uses VPLS autodiscovery to convey endpoint information. FEC 128 requires manually configured pseudowires.

The following describes the behavior of mesh groups in regards to BGP-signaled PE routers and LDP-signaled PE routers:

- BGP-signaled PE routers—Automatically discovered PE routers that use BGP for signaling are associated with the default VE mesh group. You cannot configure the Junos OS to associate these routers with a user-defined VE mesh group.
- LDP-signaled PE routers (FEC 128)—PE routers statically configured using FEC-128 LDP signaling are placed in a default mesh group. However, you can configure a VE mesh group and associate each LDP FEC-128 neighbor with it. Each configured VE mesh group contains a set of VEs that are in the same interior gateway protocol (IGP) routing instance and are fully meshed with each other in the control and data planes.
- LDP-signaled PE routers (FEC 129)—Configuration for a mesh group for FEC 129 is very similar to the configuration for FEC 128.

Note the following differences for FEC 129:

- Each user-defined mesh group must have a unique route distinguisher. Do not use the route distinguisher that is defined for the default mesh group at the **[edit routing-instances]** hierarchy level.
- Each user-defined mesh group must have its own import and export route target.
- Each user-defined mesh group can have a unique Layer 2 VPN ID. By default, all the mesh groups that are configured for the a VPLS routing-instance use the same Layer 2 VPN ID, the one that you configure at the **[edit routing-instances]** hierarchy level.

#### Related Documentation

- [Example: Configuring BGP Autodiscovery for LDP VPLS on page 725](#)

## Configuring VPLS Fast Reroute Priority

When a path is rerouted after a link failure by using the MPLS fast reroute feature, the router repairs the affected next hops by switching them from the active label switched path (LSP) to the standby LSP. To specify the order in which the router repairs next hops and restores traffic convergence for VPLS routing instances after a fast reroute event, you can use the **fast-reroute-priority** statement to configure **high**, **medium**, or **low** fast reroute priority for a VPLS routing instance. By default, the fast reroute priority for a VPLS routing instance is **low**.

The router repairs next hops and restores known unicast, unknown unicast, broadcast, and multicast traffic for VPLS routing instances in the following order, based on the fast reroute priority configuration:

1. The router repairs next hops for high-priority VPLS routing instances.
2. The router repairs next hops for medium-priority VPLS routing instances.
3. The router repairs next hops for low-priority VPLS routing instances.

Because the router repairs next hops for VPLS routing instances configured with **high** fast reroute priority first, the traffic traversing high-priority VPLS instances is restored faster than the traffic for VPLS instances configured with **medium** or **low** fast reroute priority. The ability to prioritize specific VPLS routing instances for faster convergence and traffic restoration enables service providers to offer differentiated service levels to their customers.

Within a particular fast reroute priority level (**high**, **medium**, or **low**), the router follows no particular order for traffic restoration of VPLS routing instances.



**NOTE:** VPLS fast reroute priority is not supported on EX Series switches.

To configure **high**, **medium**, or **low** fast reroute priority for a VPLS routing instance, include the **fast-reroute-priority** statement:

**fast-reroute-priority** (high | medium | low);

You can include this statement at the following hierarchy levels:

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

You can configure fast reroute priority only for routing instances with the **instance-type** set to **vpls**. If you attempt to configure fast reroute priority for a routing instance with an **instance-type** other than **vpls**, the router displays a warning message and the configuration fails.

The following example snippet shows configuration of **high** fast reroute priority for a VPLS routing instance named **test-vpls**:

```
test-vpls {
 instance-type vpls;
 forwarding-options {
 fast-reroute-priority high;
 }
}
```

To display the fast reroute priority setting configured for a VPLS routing instance, use the **show route instance detail** operational command. For information about using this command, see the [CLI Explorer](#).

## Specifying the VT Interfaces Used by VPLS Routing Instances

By default, the Junos OS automatically selects one of the virtual tunnel (VT) interfaces available to the router for de-encapsulating traffic from a remote site. The Junos OS cycles through the currently available VT interfaces, regularly updating the list of available VT interfaces as new remote sites are discovered and new connections are brought up. However, you can also explicitly configure which VT interfaces will receive the VPLS traffic.

By including the **tunnel-services** statement at the **[edit routing-instances routing-instance-name protocols vpls]** hierarchy level, you can specify that traffic for particular VPLS routing instances be forwarded to specific VT interfaces. Doing so allows you to load-balance VPLS traffic among all the available VT interfaces on the router.

The **tunnel-services** statement includes the following options:

- **devices**—Specifies the VT interfaces acceptable for use by the VPLS routing instance. If you do not configure this option, all VT interfaces available to the router can be used for de-encapsulating traffic for this instance.
- **primary**—Specifies the primary VT interface to be used by the VPLS routing instance. The VT interface specified is used to de-encapsulate all VPLS traffic from the MPLS core network for this routing instance. If the VT interface specified is unavailable, then one of the other acceptable VT interfaces (specified in the **devices** option) is used for handling the VPLS traffic. If you do not configure this option, any acceptable VT interface can be used to de-encapsulate VPLS traffic from the core.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

To specify that traffic for a particular VPLS routing instance be forwarded to specific VT interfaces, include the **tunnel-services** statement:

```
tunnel-services {
 devices device-names;
 primary primary-device-name;
}
```

These statements can be configured at the following hierarchy levels:

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

## Understanding PIM Snooping for VPLS

There are two ways to direct PIM control packets:

- By the use of PIM snooping

- By the use of PIM proxying

PIM snooping configures a device to examine and operate only on PIM hello and join/prune packets. A PIM snooping device snoops PIM hello and join/prune packets on each interface to find interested multicast receivers and populates the multicast forwarding tree with this information. PIM snooping differs from PIM proxying in that both PIM hello and join/prune packets are transparently flooded in the VPLS as opposed to the flooding of only hello packets in the case of PIM proxying. PIM snooping is configured on PE routers connected through pseudowires. PIM snooping ensures that no new PIM packets are generated in the VPLS, with the exception of PIM messages sent through LDP on pseudowires.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

A device that supports PIM snooping snoops hello packets received on attachment circuits. It does not introduce latency in the VPLS core when it forwards PIM join/prune packets.

To configure PIM snooping on a PE router, use the **pim-snooping** statement at the **[edit routing-instances instance-name protocols]** hierarchy level:

```
routing-instances {
 customer {
 instance-type vpls;
 ...
 protocols {
 pim-snooping{
 traceoptions {
 file pim.log size 10m;
 flag all;
 flag timer disable;
 }
 }
 }
 }
}
```

“[Example: Configuring PIM Snooping for VPLS](#)” on [page 581](#) explains the PIM snooping method. The use of the PIM proxying method is not discussed here and is outside the scope of this document. For more information about PIM proxying, see [PIM Snooping over VPLS](#).

#### Related Documentation

- [Example: Configuring PIM Snooping for VPLS on page 581](#)



## Example: Configuring PIM Snooping for VPLS

---

This example shows how to configure PIM snooping in a virtual private LAN service (VPLS) to restrict multicast traffic to interested devices.

- [Requirements on page 581](#)
- [Overview on page 581](#)
- [Configuration on page 582](#)
- [Verification on page 588](#)

### Requirements

This example uses the following hardware and software components:

- M Series Multiservice Edge Routers (M7i and M10i with Enhanced CFEB, M120, and M320 with E3 FPCs) or MX Series 3D Universal Edge Routers (MX80, MX240, MX480, and MX960)
- Junos OS Release 13.2 or later

### Overview

The following example shows how to configure PIM snooping to restrict multicast traffic to interested devices in a VPLS.



**NOTE:** This example demonstrates PIM snooping by the use of a PIM snooping device to restrict multicast traffic. The use of the PIM proxying method to achieve PIM snooping is out of the scope of this document and is yet to be implemented in Junos OS.

---

### Topology

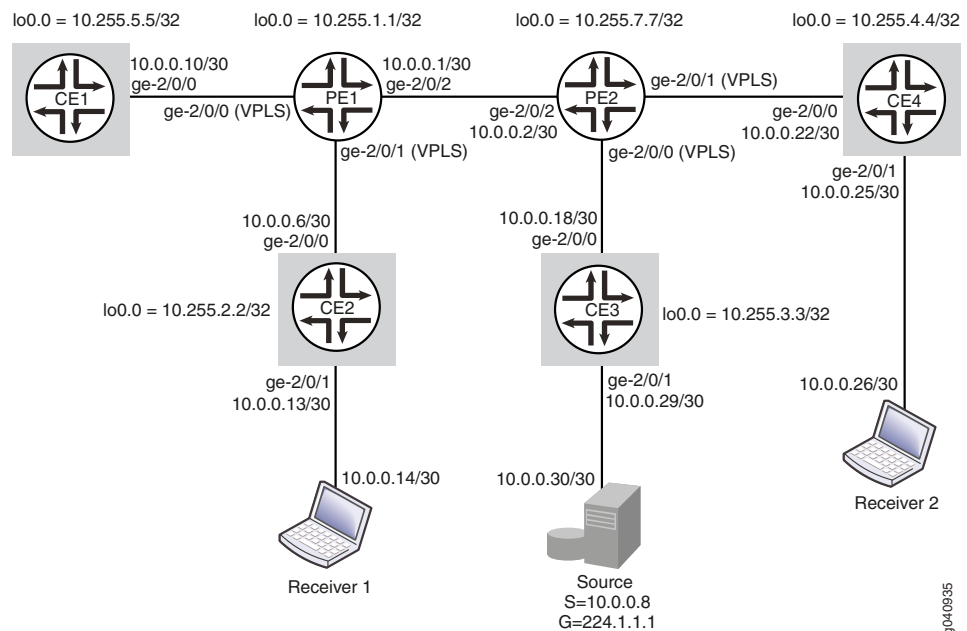
---

In this example, two PE routers are connected to each other through a pseudowire connection. Router PE1 is connected to Routers CE1 and CE2. A multicast receiver is attached to Router CE2. Router PE2 is connected to Routers CE3 and CE4. A multicast source is connected to Router CE3, and a second multicast receiver is attached to Router CE4.

PIM snooping is configured on Routers PE1 and PE2. Hence, data sent from the multicast source is received only by members of the multicast group.

[Figure 50 on page 582](#) shows the topology used in this example.

Figure 50: PIM Snooping for VPLS



## 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.

```
Router PE1
set multicast-snooping-options traceoptions file snoop.log size 10m
set interfaces ge-2/0/0 encapsulation ethernet-vpls
set interfaces ge-2/0/0 unit 0 description toCE1
set interfaces ge-2/0/1 encapsulation ethernet-vpls
set interfaces ge-2/0/1 unit 0 description toCE2
set interfaces ge-2/0/2 unit 0 description toPE2
set interfaces ge-2/0/2 unit 0 family inet address 10.0.0.1/30
set interfaces ge-2/0/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.1.1/32
set routing-options router-id 10.255.1.1
set protocols mpls interface ge-2/0/1.0
set protocols bgp group toPE2 type internal
set protocols bgp group toPE2 local-address 10.255.1.1
set protocols bgp group toPE2 family l2vpn signaling
set protocols bgp group toPE2 neighbor 10.255.7.7
set protocols ospf area 0.0.0.0 interface ge-2/0/2.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ldp interface ge-2/0/2.0
set protocols ldp interface lo0.0
set routing-instances titanium instance-type vpls
set routing-instances titanium vlan-id none
set routing-instances titanium interface ge-2/0/0.0
set routing-instances titanium interface ge-2/0/1.0
set routing-instances titanium route-distinguisher 101:101
```

```

set routing-instances titanium vrf-target target:201:201
set routing-instances titanium protocols vpls vpls-id 15
set routing-instances titanium protocols vpls site pe1 site-identifier 1
set routing-instances titanium protocols pim-snooping

Router CE1
set interfaces ge-2/0/0 unit 0 description toPE1
set interfaces ge-2/0/0 unit 0 family inet address 10.0.0.10/30
set interfaces lo0 unit 0 family inet address 10.255.2.2/32
set routing-options router-id 10.255.2.2
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols pim rp static address 10.255.3.3
set protocols pim interface all

Router CE2
set interfaces ge-2/0/0 unit 0 description toPE1
set interfaces ge-2/0/0 unit 0 family inet address 10.0.0.6/30
set interfaces ge-2/0/1 unit 0 description toReceiver1
set interfaces ge-2/0/1 unit 0 family inet address 10.0.0.13/30
set interfaces lo0 unit 0 family inet address 10.255.2.2
set routing-options router-id 10.255.2.2
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols pim rp static address 10.255.3.3
set protocols pim interface all

Router PE2
set multicast-snooping-options traceoptions file snoop.log size 10m
set interfaces ge-2/0/0 encapsulation ethernet-vpls
set interfaces ge-2/0/0 unit 0 description toCE3
set interfaces ge-2/0/1 encapsulation ethernet-vpls
set interfaces ge-2/0/1 unit 0 description toCE4
set interfaces ge-2/0/2 unit 0 description toPE1
set interfaces ge-2/0/2 unit 0 family inet address 10.0.0.2/30
set interfaces ge-2/0/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.7.7/32
set routing-options router-id 10.255.7.7
set protocols mpls interface ge-2/0/2.0
set protocols bgp group toPE1 type internal
set protocols bgp group toPE1 local-address 10.255.7.7
set protocols bgp group toPE1 family l2vpn signaling
set protocols bgp group toPE1 neighbor 10.255.1.1
set protocols ospf area 0.0.0.0 interface ge-2/0/2.0
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ldp interface ge-2/0/2.0
set protocols ldp interface lo0.0
set routing-instances titanium instance-type vpls
set routing-instances titanium vlan-id none
set routing-instances titanium interface ge-2/0/0.0
set routing-instances titanium interface ge-2/0/1.0
set routing-instances titanium route-distinguisher 101:101
set routing-instances titanium vrf-target target:201:201
set routing-instances titanium protocols vpls vpls-id 15
set routing-instances titanium protocols vpls site pe2 site-identifier 2
set routing-instances titanium protocols pim-snooping

Router CE3 (RP)
set interfaces ge-2/0/0 unit 0 description toPE2

```

```

set interfaces ge-2/0/0 unit 0 family inet address 10.0.0.18/30
set interfaces ge-2/0/1 unit 0 description toSource
set interfaces ge-2/0/1 unit 0 family inet address 10.0.0.29/30
set interfaces lo0 unit 0 family inet address 10.255.3.3/32
set routing-options router-id 10.255.3.3
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols pim rp local address 10.255.3.3
set protocols pim interface all

```

**Router CE4**

```

set interfaces ge-2/0/0 unit 0 description toPE2
set interfaces ge-2/0/0 unit 0 family inet address 10.0.0.22/30
set interfaces ge-2/0/1 unit 0 description toReceiver2
set interfaces ge-2/0/1 unit 0 family inet address 10.0.0.25/30
set interfaces lo0 unit 0 family inet address 10.255.4.4/32
set routing-options router-id 10.255.4.4
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols pim rp static address 10.255.3.3
set protocols pim interface all

```

### Configuring PIM Snooping for VPLS

#### Step-by-Step Procedure

The following example requires that you 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*.



**NOTE:** This section includes a step-by-step configuration procedure for one or more routers in the topology. For comprehensive configurations for all routers, see “CLI Quick Configuration” on page 582.

To configure PIM snooping for VPLS:

1. Configure the router interfaces forming the links between the routers.

**Router PE2**

[edit interfaces]

```

user@PE2# set ge-2/0/0 encapsulation ethernet-vpls
user@PE2# set ge-2/0/0 unit 0 description toCE3
user@PE2# set ge-2/0/1 encapsulation ethernet-vpls
user@PE2# set ge-2/0/1 unit 0 description toCE4
user@PE2# set ge-2/0/2 unit 0 description toPE1
user@PE2# set ge-2/0/2 unit 0 family mpls
user@PE2# set ge-2/0/2 unit 0 family inet address 10.0.0.2/30
user@PE2# set lo0 unit 0 family inet address 10.255.7.7/32

```



**NOTE:** ge-2/0/0.0 and ge-2/0/1.0 are configured as VPLS interfaces and connect to Routers CE3 and CE4. See *Virtual Private LAN Service Feature Guide* for more details.

**Router CE3**

[edit interfaces]

```

user@CE3# set ge-2/0/0 unit 0 description toPE2
user@CE3# set ge-2/0/0 unit 0 family inet address 10.0.0.18/30
user@CE3# set ge-2/0/1 unit 0 description toSource
user@CE3# set ge-2/0/1 unit 0 family inet address 10.0.0.29/30
user@CE3# set lo0 unit 0 family inet address 10.255.3.3/32

```



**NOTE:** The ge-2/0/1.0 interface on Router CE3 connects to the multicast source.

**Router CE4**

[edit interfaces]

```

user@CE4# set ge-2/0/0 unit 0 description toPE2
user@CE4# set ge-2/0/0 unit 0 family inet address 10.0.0.22/30
user@CE4# set ge-2/0/1 unit 0 description toReceiver2
user@CE4# set ge-2/0/1 unit 0 family inet address 10.0.0.25/30
user@CE4# set lo0 unit 0 family inet address 10.255.4.4/32

```



**NOTE:** The ge-2/0/1.0 interface on Router CE4 connects to a multicast receiver.

Similarly, configure Routers PE1, CE1, and CE2.

2. Configure the router IDs of all routers.

**Router PE2**

[edit routing-options]

```

user@PE2# set router-id 10.255.7.7

```

Similarly, configure other routers.

3. Configure an IGP on interfaces of all routers.

**Router PE2**

[edit protocols ospf area 0.0.0.0]

```

user@PE2# set interface ge-2/0/2.0
user@PE2# set interface lo0.0

```

Similarly, configure other routers.

4. Configure the LDP, MPLS, and BGP protocols on the PE routers.

**Router PE2**

[edit protocols]

```

user@PE2# set ldp interface lo0.0
user@PE2# set mpls interface ge-2/0/2.0
user@PE2# set bgp group toPE1 type internal
user@PE2# set bgp group toPE1 local-address 10.255.7.7
user@PE2# set bgp group toPE1 family l2vpn signaling
user@PE2# set bgp group toPE1 neighbor 10.255.1.1
user@PE2# set ldp interface ge-2/0/2.0

```

The BGP group is required for interfacing with the other PE router. Similarly, configure Router PE1.

5. Configure PIM on all CE routers.

Ensure that Router CE3 is configured as the rendezvous point (RP) and that the RP address is configured on other CE routers.

```
Router CE3
[edit protocols pim]
user@CE3# set rp local address 10.255.3.3
user@CE3# set interface all
```

```
Router CE4
[edit protocols pim]
user@CE4# set rp static address 10.255.3.3
user@CE4# set interface all
```

Similarly, configure Routers CE1 and CE2.

6. Configure multicast snooping options on the PE routers.

```
Router PE2
[edit multicast-snooping-options traceoptions]
user@PE2# set file snoop.log size 10m
```

Similarly, configure Router PE1.

7. Create a routing instance (**titanium**), and configure the VPLS on the PE routers.

```
Router PE2
[edit routing-instances titanium]
user@PE2# set instance-type vpls
user@PE2# set vlan-id none
user@PE2# set interface ge-2/0/0.0
user@PE2# set interface ge-2/0/1.0
user@PE2# set route-distinguisher 101:101
user@PE2# set vrf-target target:201:201
user@PE2# set protocols vpls vpls-id 15
user@PE2# set protocols vpls site pe2 site-identifier 2
```

Similarly, configure Router PE1.

8. Configure PIM snooping on the PE routers.

```
Router PE2
[edit routing-instances titanium]
user@PE2# set protocols pim-snooping
```

Similarly, configure Router PE1.

---

## Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show routing-options**, **show protocols**, **show multicast-snooping-options**, and **show routing-instances** commands.

If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@PE2# show interfaces
ge-2/0/2 {
 unit 0 {
 description toPE1
 family inet {
 address 10.0.0.2/30;
 }
 family mpls;
 }
}
ge-2/0/0 {
 encapsulation ethernet-vpls;
 unit 0 {
 description toCE3;
 }
}
ge-2/0/1 {
 encapsulation ethernet-vpls;
 unit 0 {
 description toCE4;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 10.255.7.7/32;
 }
 }
}
```

```
user@PE2# show routing-options
router-id 10.255.7.7;
```

```
user@PE2# show protocols
mpls {
 interface ge-2/0/2.0;
}
ospf {
 area 0.0.0.0 {
 interface ge-2/0/2.0;
 interface lo0.0;
 }
}
ldp {
 interface ge-2/0/2.0;
 interface lo0.0;
}
bgp {
 group toPE1 {
 type internal;
 local-address 10.255.7.7;
 family l2vpn {
 signaling;
 }
 neighbor 10.255.1.1;
 }
}
```

```
user@PE2# show multicast-snooping-options
traceoptions {
 file snoop.log size 10m;
}

user@PE2# show routing-instances
titanium {
 instance-type vpls;
 vlan-id none;
 interface ge-2/0/0.0;
 interface ge-2/0/1.0;
 route-distinguisher 101:101;
 vrf-target target:201:201;
 protocols {
 vpls {
 site pe2 {
 site-identifier 2;
 }
 vpls-id 15;
 }
 pim-snooping;
 }
}
```

Similarly, confirm the configuration on all other routers. If you are done configuring the routers, enter **commit** from configuration mode.



**NOTE:** Use the **show protocols** command on the CE routers to verify the configuration for the PIM RP .

---

## Verification

Confirm that the configuration is working properly.

- [Verifying PIM Snooping for VPLS on page 588](#)

---

### Verifying PIM Snooping for VPLS

---

**Purpose** Verify that PIM Snooping is operational in the network.

**Action** To verify that PIM snooping is working as desired, use the following commands:

- **show pim snooping interfaces**
- **show pim snooping neighbors detail**
- **show pim snooping statistics**
- **show pim snooping join**
- **show pim snooping join extensive**
- **show multicast snooping route extensive instance <instance-name> group <group-name>**



1. From operational mode on Router PE2, run the **show pim snooping interfaces** command.

```
user@PE2> show pim snooping interfaces
Instance: titanium
```

```
Learning-Domain: default
```

| Name       | State | IP | NbrCnt |
|------------|-------|----|--------|
| ge-2/0/0.0 | Up    | 4  | 1      |
| ge-2/0/1.0 | Up    | 4  | 1      |

```
DR address: 10.0.0.22
```

```
DR flooding is ON
```

The output verifies that PIM snooping is configured on the two interfaces connecting Router PE2 to Routers CE3 and CE4.

Similarly, check the PIM snooping interfaces on Router PE1.

2. From operational mode on Router PE2, run the **show pim snooping neighbors detail** command.

```
user@PE2> show pim snooping neighbors detail
```

```
Instance: titanium
```

```
Learning-Domain: default
```

```
Interface: ge-2/0/0.0
```

```
Address: 10.0.0.18
```

```
Uptime: 00:17:06
```

```
Hello Option Holdtime: 105 seconds 99 remaining
```

```
Hello Option DR Priority: 1
```

```
Hello Option Generation ID: 552495559
```

```
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
```

```
Tracking is supported
```

```
Interface: ge-2/0/1.0
```

```
Address: 10.0.0.22
```

```
Uptime: 00:15:16
```

```
Hello Option Holdtime: 105 seconds 103 remaining
```

```
Hello Option DR Priority: 1
```

```
Hello Option Generation ID: 1131703485
```

```
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
```

```
Tracking is supported
```

The output verifies that Router PE2 can detect the IP addresses of its PIM snooping neighbors (10.0.0.18 on CE3 and 10.0.0.22 on CE4).

Similarly, check the PIM snooping neighbors on Router PE1.

3. From operational mode on Router PE2, run the **show pim snooping statistics** command.

```
user@PE2> show pim snooping statistics
```

```
Instance: titanium
```

```
Learning-Domain: default
```

```
Tx J/P messages
```

```
0
```

|                              |      |
|------------------------------|------|
| RX J/P messages              | 246  |
| Rx J/P messages -- seen      | 0    |
| Rx J/P messages -- received  | 246  |
| Rx Hello messages            | 1036 |
| Rx Version Unknown           | 0    |
| Rx Neighbor Unknown          | 0    |
| Rx Upstream Neighbor Unknown | 0    |
| Rx J/P Busy Drop             | 0    |
| Rx J/P Group Aggregate       | 0    |
| Rx Malformed Packet          | 0    |
|                              |      |
| Rx No PIM Interface          | 0    |
| Rx Bad Length                | 0    |
| Rx Unknown Hello Option      | 0    |
| Rx Unknown Packet Type       | 0    |
| Rx Bad TTL                   | 0    |
| Rx Bad Destination Address   | 0    |
| Rx Bad Checksum              | 0    |
| Rx Unknown Version           | 0    |

The output shows the number of hello and join/prune messages received by Router PE2. This verifies that PIM sparse mode is operational in the network.

4. Send multicast traffic from the source terminal attached to Router CE3, for the multicast group 224.1.1.1.
5. From operational mode on Router PE2, run the **show pim snooping join**, **show pim snooping join extensive**, and **show multicast snooping route extensive instance <instance-name> group <group-name>** commands to verify PIM snooping.

```
user@PE2> show pim snooping join
Instance: titanium
Learning-Domain: default
```

```
Group: 224.1.1.1
Source: *
Flags: sparse,rptree,wildcard
Upstream neighbor: 10.0.0.18, Port: ge-2/0/0.0
```

```
Group: 224.1.1.1
Source: 10.0.0.30
Flags: sparse
Upstream neighbor: 10.0.0.18, Port: ge-2/0/0.0
```

```
user@PE2> show pim snooping join extensive
Instance: titanium
Learning-Domain: default
```

```
Group: 224.1.1.1
Source: *
Flags: sparse,rptree,wildcard
Upstream neighbor: 10.0.0.18, Port: ge-2/0/0.0
Downstream port: ge-2/0/1.0
Downstream neighbors:
10.0.0.22 State: Join Flags: SRW Timeout: 180
```

```
Group: 224.1.1.1
Source: 10.0.0.30
Flags: sparse
Upstream neighbor: 10.0.0.18, Port: ge-2/0/0.0
Downstream port: ge-2/0/1.0
```

Downstream neighbors:

10.0.0.22 State: Join Flags: S Timeout: 180

The outputs show that multicast traffic sent for the group 224.1.1.1 is sent to Receiver 2 through Router CE4 and also display the upstream and downstream neighbor details.

```
user@PE2> show multicast snooping route extensive instance titanium group 224.1.1.1
Nexthop Bulking: OFF
```

Family: INET

Group: 224.1.1.1/24

Bridge-domain: titanium

Mesh-group: \_\_all\_ces\_\_

Downstream interface list:

ge-2/0/1.0 -(1072)

Statistics: 0 kbps, 0 pps, 0 packets

Next-hop ID: 1048577

Route state: Active

Forwarding state: Forwarding

Group: 224.1.1.1/24

Source: 10.0.0.8

Bridge-domain: titanium

Mesh-group: \_\_all\_ces\_\_

Downstream interface list:

ge-2/0/1.0 -(1072)

Statistics: 0 kbps, 0 pps, 0 packets

Next-hop ID: 1048577

Route state: Active

Forwarding state: Forwarding

**Meaning** PIM snooping is operational in the network.

**Related Documentation**

- [Understanding PIM Snooping for VPLS on page 579](#)

## VPLS Label Blocks Operation

A virtual private LAN service (VPLS) is a Layer 2 (L2) service that emulates a local area network (LAN) across a wide area network (WAN). VPLS labels are defined and exchanged in the Border Gateway Protocol (BGP) control plane. In the Junos OS implementation, label blocks are allocated and used in the VPLS control plane for two primary functions: autodiscovery and signaling.

- **Autodiscovery**—A method for automatically recognizing each provider edge (PE) router in a particular VPLS domain, using BGP update messages.
- **Signaling**—Each pair of PE routers in a VPLS domain sends and withdraws VPN labels to each other. The labels are used to establish and dismantle pseudowires between the routers. Signaling is also used to transmit certain characteristics of a pseudowire.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

The PE router uses BGP extended communities to identify the members of its VPLS. Once the PE router discovers its members, it is able to establish and tear down pseudowires between members by exchanging and withdrawing labels and transmitting certain characteristics of the pseudowires.

The PE router sends common update messages to all remote PE routers, using a distinct BGP update message, thereby reducing the control plane load. This is achieved by using VPLS label blocks.

## Elements of Network Layer Reachability Information

VPLS BGP network layer reachability information (NLRI) is used to exchange VPLS membership and parameters. The elements of a VPLS BGP NLRI are defined in [Table 15 on page 592](#).

**Table 15: NLRI Elements**

| Element             | Acronym | Description                                                                                                        | Default Size (Octets) |
|---------------------|---------|--------------------------------------------------------------------------------------------------------------------|-----------------------|
| Length              |         | Total length of the NLRI size represented in bytes.                                                                | 2                     |
| Route Distinguisher | RD      | Unique identifier for each routing instance configured on a PE.                                                    | 8                     |
| VPLS Edge ID        | VE ID   | Unique number to identify the edge site.                                                                           | 2                     |
| VE Block Offset     | VBO     | Value used to identify a label block from which a label value is selected to set up pseudowires for a remote site. | 2                     |
| VE Block Size       | VBS     | Indicates the number of pseudowires that peers can have in a single block.                                         | 2                     |
| Label Base          | LB      | Starting value of the label in the advertised label block.                                                         | 3                     |

## Requirements for NLRI Elements

Junos OS requires a unique route distinguisher (RD) for each routing instance configured on a PE router. A PE router might use the same RD across a VPLS (or VPN) domain or it might use different RDs. Using different RDs helps identify the originator of the VPLS NLRI.

The VPLS edge (VE) ID can be a unique VE ID, site ID, or customer edge (CE) ID. The VE ID is used by a VPLS PE router to index into label blocks used to derive the transmit and receive VPN labels needed for transport of VPLS traffic. The VE ID identifies a particular site, so it needs to be unique within the VPLS domain, except for some scenarios such as multihoming.

All PE routers have full mesh connectivity with each other to exchange labels and set up pseudowires. The VE block size (VBS) is a configurable value that represents the number of label blocks required to cover all the pseudowires for the remote peer.

A single label block contains 8 labels (1 octet) by default. The default VBS in Junos OS is 2 blocks (2 octets) for a total of 16 labels.

### How Labels are Used in Label Blocks

Each PE router creates a mapping of the labels in the label block to the sites in a VPLS domain. A PE router advertising a label block with a block offset indicates which sites can use the labels to reach it. When a PE router is ready to advertise its membership to a VPLS domain, it allocates a label block and advertises the VPLS NLRI. In this way, other PE routers in the same VPLS domain can learn of the existence of the VPLS and set up pseudowires to it if needed. The VPLS NLRI advertised for this purpose is referred to as the *default VPLS NLRI*. The label block in the default VPLS NLRI is referred to as the *default label block*.

### Label Block Composition

A label block (set of labels) is used to reach a given site ID. A single label block contains 8 labels (1 octet) by default. The VBS is 2 octets by default in Junos OS.

The label block advertised is defined as a label base (LB) and a VE block size (VBS). It is a contiguous set of labels (LB, LB+1,...,LB+VBS-1). For example, when Router PE-A sends a VPLS update, it sends the same label block information to all other PE routers. Each PE router that receives the LB advertisement infers the label intended for Router PE-A by adding its own site ID to the label base.

In this manner, each receiving PE gets a unique label for PE-A for that VPLS. This simple method is enhanced by using a VE block offset (VBO).

A label block is defined as: <Label Base (LB), VE block offset (VBO), VE block size (VBS)> is the set {LB+VBO, LB+VBO+1,...,LB+VBO+VBS-1}.

### Label Blocks in Junos OS

Instead of a single large label block to cover all VE IDs in a VPLS, the Junos OS implementation contains several label blocks, each with a different label base. This makes label block management easier, and also allows Router PE-A to seamlessly integrate a PE router joining a VPLS with a site ID not covered by the set of label blocks that Router PE-A has already advertised.

### VPLS Label Block Structure

This section illustrates how a label block is uniquely identified.

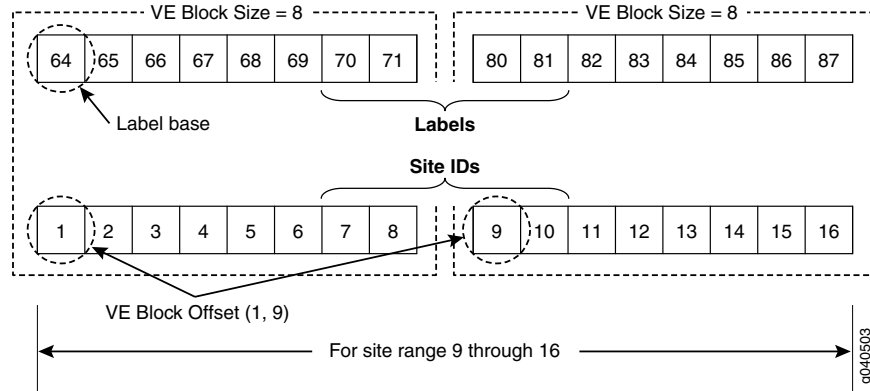
A VPLS BGP NLRI with site ID V, VE block offset VBO, VE block size VBS, and label base LB communicates the following to its peers:

- Label block for V: Labels from LB to (LB + VBS -1).
- Remote VE set for V: from VBO to (VBO + VBS -1).

The label block advertised is a set of labels used to reach a given site ID. If there are several label blocks, the remote VE set helps to identify which label block to use. The

example in [Figure 51 on page 594](#) illustrates label blocks. There are two blocks and each block has eight labels. In this example, the label values are 64 to 71 and 80 to 87.

**Figure 51: VPLS Label Block Structure**



To create a one-to-one mapping of these 16 labels to 16 sites, assume the site IDs are the numbers 1 to 16, as shown in the illustration. The site block indicates which site ID can use which label in the label block. So, in the first block, site ID 1 uses 64, site ID 2 uses 65, and so forth. Finally, site ID 8 uses 71. The 9th site ID will use the second block instead of the first block.

The labels are calculated by comparing the values of  $VBO \leq \text{Local site ID} < (VBO + VBS)$ . Consequently, site ID 9 uses 80, site ID 10 uses 81, and so on.

To further illustrate the one-to-one mapping of labels to sites, assume a label block with site offset of 1 and a label base of 10. The combination of label base and block offset contained in the VPLS NLRI provides the mapping of labels to site IDs. The block offset is the starting site ID that can use the label block as advertised in the VPLS NLRI.

To advertise the default VPLS NLRI, a PE router picks a starting block offset that fits its own site ID and is such that the end block offset is a multiple of a single label block. In Junos OS a single label block is eight labels by default.

The end block offset is the last site ID that maps to the last label in the label block. The end offset for the first block is 8 which maps to label 17 and the second block is 16. For example, a site with ID 3 picks a block offset of 1 and advertises a label block of size 8 to cover sites with IDs 1 to 8. A site with ID 10 picks a block offset of 9 to cover sites with IDs 9 to 16.

The VPLS NLRI shown in [Figure 52 on page 595](#) is for site ID 18. The label base contains value 262145. The block offset contains value 17. The illustration shows which site IDs correspond to which labels.

**Figure 52: Label Mapping Example**

VPLS NLRI for Site ID 18

|                      |
|----------------------|
| Length               |
| RD                   |
| VE ID - 18           |
| VE Block Offset - 17 |
| VE Block Size - 8    |
| Label Base - 262145  |

**Label Mapping for Site ID 18**

Label Base = 262145

**Label Block**

| Label   | 262145 | 262146 | 262147 | 262148 | 262149 | 262150 | 262151 | 262152 |
|---------|--------|--------|--------|--------|--------|--------|--------|--------|
| Site ID | 17     | 18     | 19     | 20     | 21     | 22     | 23     | 24     |

Site Offset = 17

**Site IDs**

9040504

If a PE router configured with site ID 17 is in the same VPLS domain as a PE router configured with site ID 18, it receives the VPLS NLRI as shown in Figure 2. So it uses label 262145 to send traffic to site 18. Similarly, a PE router configured with site ID 19 uses label 262147 to send traffic to a PE router configured with site ID 18. However, only PE routers configured with site IDs 17 to 24 can use the label block shown to set up pseudowires.

**Related Documentation**

- [Example: Building a VPLS From Router 1 to Router 3 to Validate Label Blocks on page 596](#)

## Configuring the Label Block Size for VPLS

---

VPLS MPLS packets have a two-label stack. The outer label is used for normal MPLS forwarding in the service provider's network. If BGP is used to establish VPLS, the inner label is allocated by a PE router as part of a label block. One inner label is needed for each remote VPLS site. Four sizes are supported. We recommend using the default size of 8, unless the network design requires a different size for optimal label usage, to allow the router to support a larger number of VPLS instances.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

If you allocate a large number of small label blocks to increase efficiency, you also increase the number of routes in the VPLS domain. This has an impact on the control plane overhead.

Changing the configured label block size causes all existing pseudowires to be deleted. For example, if you configure the label block size to be 4 and then change the size to 8, all existing label blocks of size 4 are deleted, which means that all existing pseudowires are deleted. The new label block of size 8 is created, and new pseudowires are established.

Four label block sizes are supported: 2, 4, 8, and 16. Consider the following scenarios:

- 2—Allocate the label blocks in increments of 2. For a VPLS domain that has only two sites with no future expansion plans.
- 4—Allocate the label blocks in increments of 4.
- 8 (default)—Allocate the label blocks in increments of 8.
- 16—Allocate the label blocks in increments of 16. A label block size of 16 enables you to minimize the number of routes in the VPLS domain. Use this setting only if the number of routes is the most important concern.

Configure the label block size:

```
[edit routing-instances instance-name protocols vpls]
user@router# set label-block-size 2
```

### Related Documentation

- [Configuring VPLS Routing Instances on page 563](#)

## Example: Building a VPLS From Router 1 to Router 3 to Validate Label Blocks

---

This example illustrates how VPLS label blocks are allocated for a specific configuration. It is organized in the following sections:

- [Requirements on page 597](#)
- [Overview and Topology on page 597](#)
- [Configuration on page 598](#)



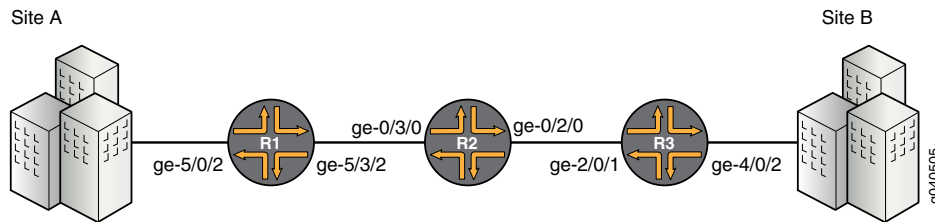
## Requirements

This configuration example requires three Juniper Networks routers.

## Overview and Topology

In the network shown in [Figure 53 on page 597](#) Router 1 is establishing a pseudowire to Router 3.

**Figure 53: Router 1 to Router 3 Topology**



Each PE filters the VPLS NLRI contained in the BGP update messages based on route target communities. Those VPLS NLRI instances that match the route target (in this case 8717:2000:2:1) are imported for further processing. The NLRI for Router 1 and Router 3 is shown in [Table 16 on page 597](#).

**Table 16: NLRI Exchange Between for Router 1 and Router 3**

| Router 1 NLRI Advertisement to Router 3 | Router 3 NLRI Advertisement to Router 1 |
|-----------------------------------------|-----------------------------------------|
| RD - 8717:1000                          | RD - 8717:1000                          |
| VE ID - 1                               | VE ID - 2                               |
| VE Block Offset - 1                     | VE Block Offset - 1                     |
| VE Block Size - 8                       | VE Block Size - 8                       |
| Label Base - 262161                     | Label Base - 262153                     |

To set up a pseudowire to Router 3, Router 1 must select a label to use to send traffic to Router 3 and also select a label that it expects Router 3 to use to send traffic to itself. The site ID contained in the VPLS NLRI from Router 3 is 2.

Router 1 learns of the existence of site ID 2 in the same VPLS domain. Using the equation  $VBO \leq \text{Local Site ID} < (VBO + VBS)$ , Router 1 checks if the route advertised by site ID 2 fits in the label block and block offset that it previously advertised to Router 3. In this example it does fit, so the site ID 2 is mapped by the VPLS NLRI advertised by Router 1, and Router 1 is ready to set up a pseudowire to Router 3.

To select the label to reach Router 3, Router 1 looks at the label block advertised by Router 3 and performs a calculation. The calculation a PE router uses to check if its site ID is mapped in the label block from the remote peer is  $VBO \leq \text{Local Site ID} < (VBO + VBS)$ . So, Router 1 selects label  $(262153 + (1 - 1)) = 262153$  to send traffic to Router 3.

Using the same equation, Router 1 looks at its own label block that it advertised and selects label  $(262161 + (2 - 1)) = 262162$  to receive traffic from Router 3. Router 1 programs its forwarding state such that any traffic destined to Router 3 carries the pseudowire label 262153 and any traffic coming from Router 3 is expected to have the pseudowire label 262162. This completes the operations on the VPLS NLRI received from Router 3. Router 1 now has a pseudowire set up to Router 3.

Router 3 operation is very similar to the Router 1 operation. Since the Router 3 site ID of 2 fits in the label block and block offset advertised by Router 1, Router 3 selects label  $(262161 + (2 - 1)) = 262162$  to send traffic to Router 1. Router 3 looks at its own label block that it advertised and selects label  $(262153 + (1 - 1)) = 262153$  to receive traffic from Router 1. This completes the creation of a pseudowire to Router 1.

By default, for VPLS operation Junos OS uses a virtual tunnel (VT) loopback interface to represent a pseudowire. This example uses a label-switched interface (LSI) instead of a VT interface because there is no change in the VPLS control plane operation. Thus, for an MX platform, if there is a tunnel physical interface card (PIC) configured, it is mandatory to include the **no-tunnel-services** statement at the **[edit routing-instances routing-instance-name protocols vpls]** hierarchy level.

## Configuration

The following sections present the steps to configure and verify the example in [Figure 53 on page 597](#).

- [Configuring Router 1 on page 598](#)
- [Configuring Router 3 on page 599](#)
- [Verifying the VPLS Label Allocations on page 600](#)

### Configuring Router 1

#### Step-by-Step Procedure

1. Configure Router 1. Create the **edut** routing instance. Specify the **vpls** instance type. Configure the route distinguisher and specify the value **8717:1000**. Configure the route target and specify the value **8717:100**. Configure the VPLS protocol. Specify **10** as the site range. Specify **1** as the site ID. Include the **no-tunnel-services** statement.

```
[edit routing-instances]
edut {
 instance-type vpls;
 interface ge-5/0/2.0;
 route-distinguisher 8717:1000;
 vrf-target target:8717:100;
 protocols {
 vpls {
 site-range 10;
 no-tunnel-services;
 site router-1 {
 site-identifier 1;
 }
 }
 }
}
```

### Configuring Router 3

- Step-by-Step Procedure**
1. Configure Router 3. Create the **edut** routing instance. Specify the **vpls** instance type. Configure the route distinguisher and specify the value **8717:2000**. Configure the route target and specify the value **8717:200**. Configure the VPLS protocol. Specify **10** as the site range. Specify **2** as the site ID. Include the **no-tunnel-services** statement.

```
[edit routing-instances]
edut {
 instance-type vpls;
 interface ge-4/0/2.0;
 route-distinguisher 8717:2000;
 vrf-target target:8717:100;
 protocols {
 vpls {
 site-range 10;
 no-tunnel-services;
 site router-3 {
 site-identifier 2;
 }
 }
 }
}
```

## Verifying the VPLS Label Allocations

- Step-by-Step Procedure**
1. As shown in the figure and the configuration, Site A is attached to Router 1. Site A is assigned a site ID of 1. Before Router 1 can announce its membership to VPLS **edut** using a BGP update message, Router 1 needs to allocate a default label block. In this example, the label base of the label block allocated by Router 1 is 262161. Since Router 1's site ID is 1, Router 1 associates the assigned label block with block offset of 1. The following messages are sent from Router 1 to Router 3 and displayed using the **monitor traffic interface interface-name** command:

```
user@Router1> monitor traffic interface ge-5/3/2
Jun 14 12:26:31.280818 BGP SEND 10.10.10.1+179 -> 10.10.10.3+53950
Jun 14 12:26:31.280824 BGP SEND message type 2 (Update) length 88
Jun 14 12:26:31.280828 BGP SEND flags 0x40 code Origin(1): IGP
Jun 14 12:26:31.280833 BGP SEND flags 0x40 code ASPath(2) length 0: <null>
Jun 14 12:26:31.280837 BGP SEND flags 0x40 code LocalPref(5): 100
Jun 14 12:26:31.280844 BGP SEND flags 0xc0 code Extended Communities(16): 2:8717:100 800a:19:0:0
Jun 14 12:26:31.280848 BGP SEND flags 0x90 code MP_reach(14): AFI/SAFI 25/65
Jun 14 12:26:31.280853 BGP SEND nhop 10.10.10.1 len 4
Jun 14 12:26:31.280862 BGP SEND 8717:1000:1:1 (label base : 262161 range : 8, ce id: 1, offset: 1)
Jun 14 12:26:31.405067 BGP RECV 10.10.10.3+53950 -> 10.10.10.1+179
Jun 14 12:26:31.405074 BGP RECV message type 2 (Update) length 88
Jun 14 12:26:31.405080 BGP RECV flags 0x40 code Origin(1): IGP
Jun 14 12:26:31.405085 BGP RECV flags 0x40 code ASPath(2) length 0: <null>
Jun 14 12:26:31.405089 BGP RECV flags 0x40 code LocalPref(5): 100
Jun 14 12:26:31.405096 BGP RECV flags 0xc0 code Extended Communities(16): 2:8717:100 800a:19:0:0
Jun 14 12:26:31.405101 BGP RECV flags 0x90 code MP_reach(14): AFI/SAFI 25/65
Jun 14 12:26:31.405106 BGP RECV nhop 10.10.10.3 len 4
Jun 14 12:26:31.405116 BGP RECV 8717:2000:2:1 (label base : 262153 range : 8, ce id: 2, offset: 1)
1)
```

2. As shown in the figure and the configuration, Site B is attached to Router 3. Site B is assigned a site ID of 2. Before Router 3 can announce its membership to VPLS **edut** using a BGP update message, Router 3 assigns a default label block with the label base of **262153**. The block offset for this label block is 1 because its own site ID of 2 fits in the block being advertised. The following messages are sent from Router 3 to Router 1 and displayed using the **monitor traffic interface interface-name** command:

```
user@Router3> monitor traffic interface ge-2/0/1
Jun 14 12:26:31.282008 BGP SEND 10.10.10.3+53950 -> 10.10.10.1+179
Jun 14 12:26:31.282018 BGP SEND message type 2 (Update) length 88
Jun 14 12:26:31.282026 BGP SEND flags 0x40 code Origin(1): IGP
Jun 14 12:26:31.282034 BGP SEND flags 0x40 code ASPath(2) length 0: <null>
Jun 14 12:26:31.282041 BGP SEND flags 0x40 code LocalPref(5): 100
Jun 14 12:26:31.282052 BGP SEND flags 0xc0 code Extended Communities(16): 2:8717:100 800a:19:0:0
Jun 14 12:26:31.282078 BGP SEND flags 0x90 code MP_reach(14): AFI/SAFI 25/65
Jun 14 12:26:31.282088 BGP SEND nhop 10.10.10.3 len 4
Jun 14 12:26:31.282102 BGP SEND 8717:2000:2:1 (label base : 262153 range : 8, ce id: 2, offset: 1)

Jun 14 12:26:31.283395 BGP RECV 10.10.10.1+179 -> 10.10.10.3+53950
Jun 14 12:26:31.283405 BGP RECV message type 2 (Update) length 88
Jun 14 12:26:31.283412 BGP RECV flags 0x40 code Origin(1): IGP
Jun 14 12:26:31.283419 BGP RECV flags 0x40 code ASPath(2) length 0: <null>
Jun 14 12:26:31.283426 BGP RECV flags 0x40 code LocalPref(5): 100
Jun 14 12:26:31.283435 BGP RECV flags 0xc0 code Extended Communities(16): 2:8717:100 800a:19:0:0
Jun 14 12:26:31.283443 BGP RECV flags 0x90 code MP_reach(14): AFI/SAFI 25/65
Jun 14 12:26:31.283471 BGP RECV nhop 10.10.10.1 len 4
```

Jun 14 12:26:31.283486 BGP RECV 8717:1000:1:1 (label base : 262161 range : 8, ce id: 1, offset: 1)

3. Verify the connection status messages for Router 1 using the **show vpls connections** command. Notice the base label is **262161**, the incoming label from Router 3 is **262162**, and the outgoing label to Router 3 is **262153**.

```
user@Router1> show vpls connections instance edut extensive
Instance: edut
 Local site: router-1 (1)
 Number of local interfaces: 1
 Number of local interfaces up: 1
 IRB interface present: no
 ge-5/0/2.0
 lsi.1049600 2 Intf - vpls edut local site 1 remote site 2
 Label-base Offset Range Preference
 262161 1 8 100
 connection-site Type St Time last up # Up trans
 2 rmt Up Jun 14 12:26:31 2009 1
 Remote PE: 10.10.10.3, Negotiated control-word: No
 Incoming label: 262162, Outgoing label: 262153
 Local interface: lsi.1049600, Status: Up, Encapsulation: VPLS
 Description: Intf - vpls edut local site 1 remote site 2
 Connection History:
 Jun 14 12:26:31 2009 status update timer
 Jun 14 12:26:31 2009 loc intf up lsi.1049600
 Jun 14 12:26:31 2009 PE route changed
 Jun 14 12:26:31 2009 Out lbl Update 262153
 Jun 14 12:26:31 2009 In lbl Update 262162
 Jun 14 12:26:31 2009 loc intf down
```

Layer-2 VPN connections:

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -< -- only outbound connection is up           |
| CN -- circuit not provisioned    | >- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unknown connection status  | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not available              |
| BK -- Backup connection          | ST -- Standby connection                       |
| PF -- Profile parse failure      | PB -- Profile busy                             |

Legend for interface status

Up -- operational  
Dn -- down

4. Verify the connection status messages for Router 3 using the **show vpls connections** command. Notice the base label is **262153**, the incoming label from Router 1 is **262153**, and the outgoing label to Router 1 is **262162**.

```
user@Router3> show vpls connections instance edut extensive
Instance: edut
 Local site: router-3 (2)
```

```

Number of local interfaces: 1
Number of local interfaces up: 1
IRB interface present: no
ge-4/0/2.0
lsi.1050368 1 Intf - vpls edut local site 2 remote site 1
Label-base Offset Range Preference
262153 1 8 100
connection-site Type St Time last up # Up trans
1 rmt Up Jun 14 12:26:31 2009 1
 Remote PE: 10.10.10.1, Negotiated control-word: No
 Incoming label: 262153, Outgoing label: 262162
 Local interface: lsi.1050368, Status: Up, Encapsulation: VPLS
 Description: Intf - vpls edut local site 2 remote site 1
Connection History:
 Jun 14 12:26:31 2009 status update timer
 Jun 14 12:26:31 2009 loc intf up lsi.1050368
 Jun 14 12:26:31 2009 PE route changed
 Jun 14 12:26:31 2009 Out lbl Update 262162
 Jun 14 12:26:31 2009 In lbl Update 262153
 Jun 14 12:26:31 2009 loc intf down

```

#### Layer-2 VPN connections:

##### Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -< -- only outbound connection is up           |
| CN -- circuit not provisioned    | >- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unknown connection status  | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not available              |
| BK -- Backup connection          | ST -- Standby connection                       |
| PF -- Profile parse failure      | PB -- Profile busy                             |

##### Legend for interface status

Up -- operational  
Dn -- down

**Related** • [VPLS Label Blocks Operation on page 591](#)  
**Documentation**

# Associating Interfaces with VPLS

- [Configuring Interfaces for VPLS Routing on page 603](#)
- [VPLS and Aggregated Ethernet Interfaces on page 609](#)
- [Enabling VLAN Tagging on page 610](#)
- [Configuring VPLS Without a Tunnel Services PIC on page 611](#)

## Configuring Interfaces for VPLS Routing

---

On each PE router and for each VPLS routing instance, specify which interfaces are intended for the VPLS traffic traveling between PE and CE routers. To specify the interface for VPLS traffic, include the **interface** statement in the routing instance configuration:

```
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*]

You must also define each interface by including the following statements:

```
vlan-tagging vlan-tagging;
encapsulation encapsulation-type;
unit logical-unit-number {
 family vpls;
 vlan-id vlan-id-number;
}
```

You can include these statements at the following hierarchy levels:

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



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

The following sections provide enough information to enable you to configure interfaces for VPLS routing.

- [Configuring the VPLS Interface Name on page 604](#)
- [Configuring VPLS Interface Encapsulation on page 604](#)
- [Enabling VLAN Tagging on page 606](#)
- [Configuring VLAN IDs for Logical Interfaces on page 607](#)
- [Enabling VLANs for Hub and Spoke VPLS Networks on page 608](#)
- [Configuring Aggregated Ethernet Interfaces for VPLS on page 608](#)

## Configuring the VPLS Interface Name

Specify both the physical and logical portions of the interface name, in the following format:

*physical.logical*

For example, in **ge-1/2/1.2**, **ge-1/2/1** is the physical portion of the interface name and **2** is the logical portion. If you do not specify the logical portion of the interface name, **0** is set by default.

A logical interface can be associated with only one routing instance.

If you enable a routing protocol on all instances by specifying **interfaces all** when configuring the master instance of the protocol at the **[edit protocols]** hierarchy level, and you configure a specific interface for VPLS routing at the **[edit routing-instances routing-instance-name]** hierarchy level, the latter interface statement takes precedence and the interface is used exclusively for VPLS.

If you explicitly configure the same interface name at both the **[edit protocols]** and **[edit routing-instances routing-instance-name]** hierarchy levels and then attempt to commit the configuration, the commit operation fails.

## Configuring VPLS Interface Encapsulation

You need to specify an encapsulation type for each PE-router-to-CE-router interface configured for VPLS. This section describes the **encapsulation** statement configuration options available for VPLS.

To configure the encapsulation type on the physical interface, include the **encapsulation** statement:

**encapsulation** (ethernet-vpls | ether-vpls-over-atm-llc | extended-vlan-vpls | vlan-vpls);

You can include the **encapsulation** statement for physical interfaces at the following hierarchy levels:

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



You can configure the following physical interface encapsulations for VPLS routing instances:

- **ethernet-vpls**—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VLAN 802.1Q tagging and VPLS enabled. The PE router expects to receive Ethernet frames with VLAN tags that are not service-delimiting. The Ethernet frames are not meaningful to the PE router and cannot be used by the service provider to separate customer traffic.

On M Series routers (except the M320 router), the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.

- **ether-vpls-over-atm-llc**—For ATM intelligent queuing (IQ) interfaces only, use the Ethernet virtual private LAN service (VPLS) over ATM LLC encapsulation to bridge Ethernet interfaces and ATM interfaces over a VPLS routing instance (as described in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*). Packets from the ATM interfaces are converted to standard ENET2/802.3 encapsulated Ethernet frames with the frame check sequence (FCS) field removed.
- **extended-vlan-vpls**—Use extended virtual LAN (VLAN) VPLS encapsulation on Ethernet interfaces that have VLAN 802.1Q tagging and VPLS enabled and that must accept packets carrying TPIDs 0x8100, 0x9100, and 0x9901. On M Series routers (except the M320 router), the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.



**NOTE:** The built-in Gigabit Ethernet PIC on an M7i router does not support extended VLAN VPLS encapsulation.

- **vlan-vpls**—Use VLAN VPLS encapsulation on Ethernet interfaces with VLAN 802.1Q tagging and VPLS enabled. The PE router expects to receive Ethernet frames with VLAN tags that are service-delimiting. These VLAN tags can be used by the service provider to separate customer traffic. For example, LAN traffic from different customers can flow through the same service provider switch, which can then apply VLAN tags to distinguish one customer's traffic from the others. The traffic can then be forwarded to the PE router.

Interfaces with VLAN VPLS encapsulation accept packets carrying standard TPID values only. On M Series routers (except the M320 router), the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.

To configure the encapsulation type for logical interfaces, include the **encapsulation** statement:

```
encapsulation (ether-vpls-over-atm-llc | vlan-vpls);
```

You can include the **encapsulation** statement for logical interfaces at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *number*]**

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

You can configure the following logical interface encapsulations for VPLS routing instances:

- **ether-vpls-over-atm-llc**—Use Ethernet VPLS over Asynchronous Transfer Mode (ATM) logical link control (LLC) encapsulation to bridge Ethernet interfaces and ATM interfaces over a VPLS routing instance (as described in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*). Packets from the ATM interfaces are converted to standard ENET2/802.3-encapsulated Ethernet frames with the frame check sequence (FCS) field removed. This encapsulation type is supported on ATM intelligent queuing (IQ) interfaces only.
- **vlan-vpls**—Use VLAN VPLS encapsulation on Ethernet interfaces with VLAN 802.1Q tagging and VPLS enabled. The PE router expects to receive Ethernet frames with VLAN tags that are service-delimiting. These VLAN tags can be used by the service provider to separate customer traffic. For example, LAN traffic from different customers can flow through the same service provider switch, which can then apply VLAN tags to distinguish one customer's traffic from the others. The traffic can then be forwarded to the PE router.

Interfaces with VLAN VPLS encapsulation accept packets carrying standard TPID values only. On M Series routers (except the M320 router), the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.



**NOTE:** Label-switched interfaces (LSIs) do not support VLAN VPLS encapsulation. Therefore, you can only use VLAN VPLS encapsulation on a PE-router-to-CE-router interface and not a core-facing interface.

When you configure the physical interface encapsulation as **vlan-vpls**, you also need to configure the same interface encapsulation for the logical interface. You need to configure the **vlan-vpls** encapsulation on the logical interface because the **vlan-vpls** encapsulation allows you to configure a mixed mode, where some of the logical interfaces use regular Ethernet encapsulation (the default for logical interfaces) and some use **vlan-vpls**.



**NOTE:** Starting with Junos OS release 13.3, a commit error occurs when you configure **vlan-vpls** encapsulation on a physical interface and configure **family inet** on one of the logical units. Previously, it was possible to commit this invalid configuration.

## Enabling VLAN Tagging

Junos OS supports receiving and forwarding routed Ethernet frames with 802.1Q virtual local area network (VLAN) tags and running the Virtual Router Redundancy Protocol (VRRP) over 802.1Q-tagged interfaces. For VPLS to function properly, configure the router to receive and forward frames with 802.1Q VLAN tags by including the **vlan-tagging** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]
vlan-tagging;
```

Gigabit Ethernet interfaces can be partitioned. You can assign up to 4095 different logical interfaces, one for each VLAN, but you are limited to a maximum of 1024 VLANs on any single Gigabit Ethernet or 10-Gigabit Ethernet port. Fast Ethernet interfaces can also be partitioned, with a maximum of:

- 1024 logical interfaces for the 4-port FE PIC
- 1024 logical interfaces for the 2-port Fixed Interface Card (FIC) on an M7i router
- 16 logical interfaces for the M40e router

Table 17 on page 607 lists VLAN ID ranges by interface type.

**Table 17: VLAN ID Range by Interface Type**

| Interface Type   | VLAN ID Range    |
|------------------|------------------|
| Fast Ethernet    | 512 through 1023 |
| Gigabit Ethernet | 512 through 4094 |

## Configuring VLAN IDs for Logical Interfaces

You can bind a VLAN identifier to a logical interface by including the **vlan-id** statement:

```
vlan-id number;
```

You can include this statement at the following hierarchy levels:

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

You can also configure a logical interface to forward packets and learn MAC addresses within each VPLS routing instance configured with a VLAN ID that matches a VLAN ID specified in a list using the **vlan-id-list** statement. VLAN IDs can be entered individually using a space to separate each ID, entered as an inclusive list separating the starting VLAN ID and ending VLAN ID with a hyphen, or a combination of both.

For example, to configure the VLAN IDs 20 and 45 and the range of VLAN IDs between 30 and 40, issue the following command from the CLI:

```
set interfaces ge-1/0/1 unit 1 vlan-id-list [20 30-40 45];
```

To configure a list of VLAN IDs for a logical interface, include the **vlan-id-list** statement:

```
vlan-id-list list-of-vlan-ids;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]

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

## Enabling VLANs for Hub and Spoke VPLS Networks

For hub and spoke VPLS networks, you need to configure the **swap** option for the **output-vlan-map** statement on the hub facing interface of each spoke PE router. The **output-vlan-map** statement ensures that the vlan ID of the spoke PE router matches the VLAN ID of the hub PE router in the VPLS network. The following configuration example illustrates an interface configuration with the output-vlan-map statement included:

```
[edit interfaces xe-4/0/0]
vlan-tagging;
encapsulation flexible-ethernet-services;
unit 610 {
 encapsulation vlan-ccc;
 vlan-id 610;
 output-vlan-map swap;
}
```

## Configuring Aggregated Ethernet Interfaces for VPLS

You can configure aggregated Ethernet interfaces between CE devices and PE routers for VPLS routing instances. Traffic is load-balanced across all of the links in the aggregated interface. If one or more links in the aggregated interface fails, the traffic is switched to the remaining links.

For more information about how aggregated Ethernet interfaces function in the context of VPLS, see [“VPLS and Aggregated Ethernet Interfaces” on page 609](#).

To configure aggregated Ethernet interfaces for VPLS, configure the interface for the VPLS routing instance as follows:

```
interfaces aex {
 vlan-tagging;
 encapsulation encapsulation-type;
 unit logical-unit-number {
 vlan-id number;
 }
}
```

You can configure the following physical link-layer encapsulation types for the VPLS aggregated Ethernet interface:

- **ethernet-vpls**
- **extended-vlan-vpls**
- **flexible-ethernet-services**
- **vlan-vpls**

For the **interface** configuration statement, in **aex**, the **x** represents the interface instance number to complete the link association; **x** can be from 0 through 127, for a total of 128 aggregated interfaces.

For more information about how to configure aggregated Ethernet interfaces, see the *Ethernet Interfaces Feature Guide for Routing Devices*.

The aggregated Ethernet interface must also be configured for the VPLS routing instance as shown in the following example:

```
[edit]
routing-instances {
 green {
 instance-type vpls;
 interface ae0.0;
 route-distinguisher 10.255.234.34:1;
 vrf-target target:11111:1;
 protocols {
 vpls {
 site-range 10;
 site green3 {
 site-identifier 3;
 }
 }
 }
 }
}
```

Interface **ae0.0** represents the aggregated Ethernet interface in the routing instance configuration. The VPLS routing instance configuration is otherwise standard.

## VPLS and Aggregated Ethernet Interfaces

You can configure aggregated Ethernet interfaces between CE devices and PE routers for VPLS routing instances. Traffic is load-balanced across all of the links in the aggregated interface. If one or more links in the aggregated interface fails, the traffic is switched to the remaining links.

Forwarding is based on a lookup of the DA MAC address. For the remote site, if a packet needs to be forwarded over an LSP, the packet is encapsulated and forwarded through the LSP. If the packet destination is a local site, it is forwarded over appropriate local site interface. For an aggregated Ethernet interface on the local site, packets are sent out of the load-balanced child interface. The Packet Forwarding Engine acquires the child link to transmit the data.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

When a received packet does not have a match to a MAC address in the forwarding database, the packet is forwarded over a set of interfaces determined from a lookup in the flooding database based on the incoming interface. This is denoted by a flood next hop. The flood next hop can include the aggregated Ethernet interface as the set of interfaces to flood the packet.

Each VPLS routing instance configured on a PE router has its own forwarding database entries that associate all of the MAC addresses the VPLS routing instance acquires with each corresponding port. A route is added to the kernel with a MAC address as the prefix and the next hop used to reach the destination. The route is an interface if the destination is local. For a remote destination, the route is a next hop for the remote site.

For local aggregated Ethernet interfaces on M Series and T Series routers, learning is based on the parent aggregated Ethernet logical interface. To age out MAC addresses for aggregated Ethernet interfaces, each Packet Forwarding Engine is queried to determine where the individual child interfaces are located. MAC addresses are aged out based on the age of the original interface.

For MX Series routers and EX Series switches, when a Dense Port Concentrator (DPC) learns a MAC address it causes the Routing Engine to age out the entry. This behavior applies to all logical interfaces. For an aggregated Ethernet logical interface, once all the member DPCs have aged out the entry, the entry is deleted from the Routing Engine.

**Related  
Documentation**

- [Configuring Interfaces for VPLS Routing on page 603](#)
- [Configuring Aggregated Ethernet Interfaces for VPLS on page 608](#)

## Enabling VLAN Tagging

Junos OS supports receiving and forwarding routed Ethernet frames with 802.1Q virtual local area network (VLAN) tags and running the Virtual Router Redundancy Protocol (VRRP) over 802.1Q-tagged interfaces. For VPLS to function properly, configure the router to receive and forward frames with 802.1Q VLAN tags by including the **vlan-tagging** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]
vlan-tagging;
```

Gigabit Ethernet interfaces can be partitioned. You can assign up to 4095 different logical interfaces, one for each VLAN, but you are limited to a maximum of 1024 VLANs on any single Gigabit Ethernet or 10-Gigabit Ethernet port. Fast Ethernet interfaces can also be partitioned, with a maximum of:

- 1024 logical interfaces for the 4-port FE PIC
- 1024 logical interfaces for the 2-port Fixed Interface Card (FIC) on an M7i router
- 16 logical interfaces for the M40e router

[Table 17 on page 607](#) lists VLAN ID ranges by interface type.

**Table 18: VLAN ID Range by Interface Type**

| Interface Type   | VLAN ID Range    |
|------------------|------------------|
| Fast Ethernet    | 512 through 1023 |
| Gigabit Ethernet | 512 through 4094 |

## Configuring VPLS Without a Tunnel Services PIC

VPLS normally uses a dynamic virtual tunnel logical interface on a Tunnel Services PIC to model traffic from a remote site (a site on a remote PE router that is in a VPLS domain). All traffic coming from a remote site is treated as coming in over the virtual port representing this remote site, for the purposes of Ethernet flooding, forwarding, and learning. An MPLS lookup based on the inner VPN label is done on a PE router. The label is stripped and the Layer 2 Ethernet frame contained within is forwarded to a Tunnel Services PIC. The PIC loops back the packet and then a lookup based on Ethernet MAC addresses is completed. This approach requires that the router have a Tunnel Services PIC and that the PE router complete two protocol lookups.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

You can configure VPLS without a Tunnel Services PIC by configuring the **no-tunnel-services** statement. This statement creates a label-switched interface (LSI) to provide VPLS functionality. An LSI MPLS label is used as the inner label for VPLS. This label maps to a VPLS routing instance. On the PE router, the LSI label is stripped and then mapped to a logical LSI interface. The Layer 2 Ethernet frame is then forwarded using the LSI interface to the correct VPLS routing instance.

By default, VPLS requires a Tunnel Services PIC. To configure VPLS on a router without a Tunnel Services PIC and create an LSI, include the **no-tunnel-services** statement:

```
no-tunnel-services;
```

For a list of the hierarchy levels at which you can include this statement, see the summary section for this statement.

To configure a VPLS routing instance on a router without a tunnel services PIC, include the **no-tunnel-services** statement at the **[edit routing-instances routing-instance-name protocols vpls]** hierarchy level. To configure static VPLS on a router without a tunnel services PIC, include the **no-tunnel-services** statement at the **[edit protocols vpls static-vpls]** hierarchy level.

When you configure VPLS without a Tunnel Services PIC by including the **no-tunnel-services** statement, the following limitations apply:

- An Enhanced FPC is required.
- ATM1 interfaces are not supported.
- Aggregated SONET/SDH interfaces are not supported as core-facing interfaces.
- Channelized interfaces are not supported as core-facing interfaces.
- GRE-encapsulated interfaces are not supported as core-facing interfaces.

- Related Documentation**
- [Configuring Static Pseudowires for VPLS on page 613](#)



# Configuring Pseudowires

- [Configuring Static Pseudowires for VPLS on page 613](#)
- [VPLS Path Selection Process for PE Routers on page 615](#)
- [BGP and VPLS Path Selection for Multihomed PE Routers on page 617](#)
- [Dynamic Profiles for VPLS Pseudowires on page 619](#)
- [Use Cases for Dynamic Profiles for VPLS Pseudowires on page 620](#)
- [Example: Configuring VPLS Pseudowires with Dynamic Profiles—Basic Solutions on page 620](#)
- [Example: Configuring VPLS Pseudowires with Dynamic Profiles—Complex Solutions on page 625](#)
- [Configuring the FAT Flow Label for FEC 128 VPLS Pseudowires for Load-Balancing MPLS Traffic on page 629](#)
- [Configuring the FAT Flow Label for FEC 129 VPLS Pseudowires for Load-Balancing MPLS Traffic on page 631](#)
- [Example: Configuring H-VPLS BGP-Based and LDP-Based VPLS Interoperation on page 632](#)
- [Example: Configuring BGP-Based H-VPLS Using Different Mesh Groups for Each Spoke Router on page 653](#)
- [Example: Configuring LDP-Based H-VPLS Using a Single Mesh Group to Terminate the Layer 2 Circuits on page 675](#)
- [Example: Configuring H-VPLS With VLANs on page 681](#)
- [Example: Configuring H-VPLS Without VLANs on page 693](#)

## Configuring Static Pseudowires for VPLS

---

You can configure a VPLS domain using static pseudowires. A VPLS domain consists of a set of PE routers that act as a single virtual Ethernet bridge for the customer sites connected to these routers. By configuring static pseudowires for the VPLS domain, you do not need to configure the LDP or BGP protocols that would normally be used for signaling. However, if you configure static pseudowires, any changes to the VPLS network topology have to be managed manually.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

Static pseudowires require that you configure a set of in and out labels for each pseudowire configured for the VPLS domain. You still need to configure a VPLS identifier and neighbor identifiers for a static VPLS domain. You can configure both static and dynamic neighbors within the same VPLS routing instance.

To configure a static pseudowire for a VPLS neighbor, include the **static** statement:

```
static (Protocols VPLS) {
 incoming-label label;
 outgoing-label label;
}
```

You must configure an incoming and outgoing label for the static pseudowire using the **incoming-label** and **outgoing-label** statements. These statements identify the static pseudowire's incoming traffic and destination.

To configure a static pseudowire for a VPLS neighbor, include the **static** statement at the **[edit routing-instances routing-instance-name protocols vpls neighbor address]** hierarchy level.

You can also configure the **static** statement for a backup neighbor (if you configure the neighbor as static the backup must also be static) by including it at the **[edit routing-instances routing-instance-name protocols vpls neighbor address backup-neighbor address]** hierarchy level and for a mesh group by including it at the **[edit routing-instances routing-instance-name protocols vpls mesh-group mesh-group-name neighbor address]** hierarchy level.

For a list of hierarchy levels at which you can include the **static** statement, see the statement summary section for this statement.

To enable static VPLS on a router, you need to either configure a virtual tunnel interface (requires the router to have a tunnel services PIC) or you can configure a label switching interface (LSI). To configure an LSI, include the **no-tunnel-services** statement at the **[edit protocols vpls static-vpls]** hierarchy level. For more information, see [“Configuring VPLS Without a Tunnel Services PIC” on page 611](#).



**NOTE:** Static pseudowires for VPLS using an LSI is supported on MX series routers and EX Series switches only. For M series and T series routers, a tunnel services PIC is required.

If you issue a **show vpls connections** command, static neighbors are displayed with **"SN"** next to their addresses in the command output.

#### Related Documentation

- [Configuring VPLS Without a Tunnel Services PIC on page 611](#)

## VPLS Path Selection Process for PE Routers

The VPLS path selection process is used to select the best path between a remote PE router and a local PE router in a VPLS network. This path selection process is applied to routes received from both single-homed and multi-homed PE routers.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

When the VPLS path selection process is complete, a PE router is made the designated VPLS edge (VE) device. The designated VE device effectively acts as the endpoint for the VPLS pseudowire that is signaled from the remote PE router. Once a PE router is made the designated VE device, a pseudowire can be signaled between the remote PE router and the local PE router and then VPLS packets can begin to flow between the PE routers.

Routes from multihomed PE routers connected to the same customer site share the same site ID, but can have different route distinguishers and block offsets. You can alter the configurations of the route distinguishers and block offsets to make a router more likely or less likely to be selected as the designated VE device.

On each PE router in the VPLS network, the best path to the CE device is determined by completing the following VPLS path selection process on each route advertisement received:

1. If the advertisement has the down bit set to 0, the advertisement is discarded.
2. Select the path with a higher preference. The preference attribute is obtained from the site-preference configured using the **site-preference** statement at the **[edit routing-instances routing-instance-name protocols vpls site site-name]** hierarchy level. If the site preference is 0, the preference attribute is obtained from the local preference.
3. If the preference values are the same, select the path with the lower router ID.
4. If the router IDs are the same, the routes are from the same PE router and the advertisement is considered to be an update. The router ID corresponds to the value of the originator ID for the BGP attribute (if present). Otherwise, the IP address for the remote BGP peer is used.
5. If the block offset values are the same, the advertisement is considered to be an update.

Once the VPLS path selection process has been completed and the designated VE device has been selected, a pseudowire is signaled between the remote PE router and the local PE router.



**NOTE:** The VPLS path selection process works the same whether or not the route has been received from another PE router, a route reflector, or an autonomous system border router (ASBR).

When the remote PE router establishes or refreshes a pseudowire to the local PE router, it verifies that the prefix is in the range required for the site ID based on the block offset and label range advertised by the designated VE device. If the prefix is out of range, the pseudowire status is set to out of range.

The following cases outline the potential decisions that could be made when a PE router completes the VPLS path selection process for a Layer 2 advertisement in the VPLS network:

- The PE router originated one of the advertisements and selected its own advertisement as the best path.

This PE router has been selected as the designated VE device. Selection as the designated VE device triggers the creation of pseudowires to and from the other PE routers in the VPLS network. If the remote customer site is multihomed, the designated VE device triggers the creation of pseudowires to and from only the designated VE device for the remote site.

- The PE router originated one of the advertisements but did not select its own advertisement as the best path.

This PE router is a redundant PE router for a multihomed site, but it was not selected as the designated VE device. However, if this PE router has just transitioned from being the designated VE device (meaning it was receiving traffic from the remote PE routers addressed to the multihomed customer site), the PE router tears down all the pseudowires that it had to and from the other PE routers in the VPLS network.

- The PE router received the route advertisements and selected a best path. It did not originate any of these advertisements because it was not connected to the customer site.

If the best path to the customer site (the designated VE device) has not changed, nothing happens. If the best path has changed, this PE router brings up pseudowires to and from the newly designated VE device and tears down the pseudowires to and from the previously designated VE device.

If this PE router does not select a best path after running the VPLS path selection process, then the local PE router does not consider the remote site to exist.

When a VE device receives an advertisement for a Layer 2 NLRI that matches its own site ID but the site is not multihomed, the pseudowire between the VE device and the transmitting PE router transitions to a site collision state and is not considered to be up.

**Related  
Documentation**

- [BGP Route Reflectors for VPLS on page 552](#)

## BGP and VPLS Path Selection for Multihomed PE Routers

The BGP and VPLS path selection procedures are used to select the best path between the remote PE router and one of the multihomed PE routers. As part of these path selection procedures, one of the multihomed PE routers is made the designated VE device. The designated VE device effectively acts as the endpoint for the VPLS pseudowire from the remote PE router. Once a multihomed PE router is made the designated VE device, a pseudowire can be created between the remote PE router and the multihomed PE router.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

Routes from multihomed PE routers connected to the same customer site share the same site ID, but can have different route distinguishers and block offsets. On each PE router in the VPLS network, the best path to the multihomed PE router is determined by completing the following VE device-selection procedures on each route advertisement received from a multihomed PE router:

1. BGP designated VE device-selection procedure—Runs before the VPLS designated VE device-selection procedure. However, the BGP designated VE device-selection procedure is used only when the route distinguishers for the multihomed PE routers are identical. If the route distinguishers are unique, only the VPLS designated VE device-selection procedure is run.
2. VPLS designated VE device-selection procedure—Runs after the BGP designated VE device-selection procedure. However, if the route distinguishers for each multihomed PE router are unique, the advertisements are not considered relevant to the BGP designated VE device-selection procedure. As a consequence, only the VPLS designated VE device-selection procedure is used.

The BGP designated VE device-selection procedure is as follows:

1. If the advertisement has the down bit set to 0, the advertisement is discarded.
2. Select the path with a higher preference. The preference attribute is obtained from the site-preference configured using the **site-preference** statement at the [edit routing-instances *routing-instance-name* protocols vpls site *site-name*] hierarchy level. If the site-preference is 0, the preference attribute is obtained from the local-preference.
3. If the preference values are the same, select the path with the lower router-id.
4. If the router-ids are the same, the routes are from the same PE router and the advertisement is considered to be an update.

Once the BGP designated VE device-selection procedure is complete, the VPLS designated VE device-selection procedure begins. This procedure is carried out regardless of the outcome of the BGP designated VE device-selection procedure:

1. If the advertisement has the down bit set to 0, the advertisement is discarded.
2. Select the path with a higher preference. The preference attribute is obtained from the site-preference configured using the **site-preference** statement at the [edit routing-instances *routing-instance-name* protocols vpls site *site-name*] hierarchy level. If the site-preference is 0, the preference attribute is obtained from the local-preference.
3. If the preference values are the same, select the path with the lower router-id.
4. If the router-ids are the same, select the path with a lower route distinguisher.
5. If the route distinguishers are the same, select the path with the lower block offset value.
6. If the block offset values are the same, the advertisement is considered to be an update.

Once the BGP and VPLS path selection procedures have been completed and the designated VE devices have been selected, a pseudowire can be created between the remote PE router and the multihomed PE router.

When the remote PE router establishes or refreshes a pseudowire to the local PE router, it verifies that the prefix is in the range required for the site ID based on the block offset and label range advertised by the designated VE device. If the prefix is out of range, the pseudowire status is set to out of range.

The following cases outline the potential decisions that could be made when a PE router completes the BGP and VPLS path selection procedures for a Layer 2 advertisement in the VPLS network:

- The PE router originated one of the multihomed advertisements and selected its own advertisement as the best path.

This PE router has been selected as the designated VE device. Selection as the designated VE device triggers the creation of pseudowires to and from the other PE routers in the VPLS network. When the remote customer site is also multihomed, the designated VE device triggers the creation of pseudowires to and from only the designated VE device for the remote site.

- The PE router originated one of the multihomed advertisements but did not select its own advertisement as the best path.

This PE router is one of the redundant PE routers for the multihomed site; it was not selected as the designated VE device. However, if this PE router has just transitioned from being the designated VE device (meaning it was receiving traffic from the remote PE routers addressed to the multihomed customer site), the PE router tears down all the pseudowires that it had to and from the other PE routers in the VPLS network.

- The PE router receives the multihomed advertisements and selects a best path; it does not originate any of these advertisements because it is not connected to the multihomed customer site.

If the preferred path to the customer site (the designated VE device) has not changed, nothing happens. If the preferred path has changed, this PE router brings up pseudowires to and from the newly designated VE device and tears down the pseudowires to and from the previously designated VE device.

If this PE router does not select a best path after running the BGP and VPLS path selection process, the local PE router does not consider the remote site to exist.

When a VE device receives an advertisement for a Layer 2 NLRI which matches its own site ID but the site is not multihomed, the pseudowire between it and the transmitting PE router transitions to a site collision state and is not considered to be up.

---

## Dynamic Profiles for VPLS Pseudowires

---

A router often has two types of interfaces:

- Static interfaces, which are configured before the router is booted
- Dynamic interfaces, which are created after the router is booted and while it is running

A virtual private LAN service (VPLS) pseudowire interface (such as **lsi.1048576**) is dynamically created by the system. Therefore, the logical interface unit number for the VPLS pseudowire is not available in advance to configure characteristics such as virtual local area network (VLAN) identifiers and other parameters. As a result, certain VLAN manipulation features that are easily applied to static interfaces (such as **xe-**, **ge-**, and so on) are either not supported on dynamic interfaces or supported in a nonstandard method.

However, on MX Series routers, there is another configuration method that dynamic interfaces can use to determine their VLAN parameters when they are created by a running router: *dynamic profiles*. A dynamic profile is a conceptual container that includes parameters associated with a dynamic entity, parameters whose values are not known at the time the entity is configured.

A dynamic profile acts as a kind of template that enables you to create, update, or remove a configuration that includes client access (for example, interface or protocol) or service (for example, CoS) attributes. Using these profiles you can consolidate all of the common attributes of a client (and eventually a group of clients) and apply the attributes simultaneously. The router contains several predefined variables that enable dynamic association of interfaces and logical units to incoming subscriber requests. While configuring a dynamic profile, use the **\$junos-interface-ifd-name** variable for a dynamic physical interface and the **\$junos-underlying-unit-number** variable for a dynamic logical interface (unit). When a client accesses the router, the dynamic profile configuration replaces the predefined variable with the actual interface name or unit value for the interface the client is accessing.

Dynamic profiles for VPLS are supported only on MX Series routers. For more information about dynamic profiles, see the *Junos OS Broadband Subscriber Management and Services Library*.

**Related  
Documentation**

- *Ethernet Networking Feature Guide for MX Series Routers*
- *Dynamic Profiles Overview*
- [Use Cases for Dynamic Profiles for VPLS Pseudowires on page 620](#)
- [Example: Configuring VPLS Pseudowires with Dynamic Profiles—Basic Solutions on page 620](#)
- [Example: Configuring VPLS Pseudowires with Dynamic Profiles—Complex Solutions on page 625](#)

---

## Use Cases for Dynamic Profiles for VPLS Pseudowires

A dynamic profile is a set of characteristics, defined in a type of template, that you can use to provide dynamic subscriber access and services for broadband applications. These services are assigned dynamically to interfaces. You can use dynamic profiles to configure the VLAN parameters of the dynamic interfaces on MX Series routers.

Two use cases for configuring VPLS pseudowires with dynamic profiles are:

- **Configuring an extra VLAN tag onto pseudowire traffic** — This is a common scenario where all the traffic received from a customer edge (CE) interface needs an additional VLAN tag toward the core. In such cases, you can use dynamic profiles at ingress and egress to control the pseudowire behavior. You can apply dynamic profiles to receive the desired frames, set the additional VLAN tag for these frames, and send these tagged frames with the desired VLAN identifier.
- **Configuring a VPLS pseudowire as a trunk interface** — This is another common scenario where the requirement is to accept traffic from a particular source and to route the traffic based on specific criteria. Dynamic profiles can be used to create multiple pseudowire trunk interfaces to accept the traffic based on specific VLAN identifiers, and to route the accepted traffic to the desired destination.

**Related  
Documentation**

- *Dynamic Profiles Overview*
- [Dynamic Profiles for VPLS Pseudowires on page 619](#)

---

## Example: Configuring VPLS Pseudowires with Dynamic Profiles—Basic Solutions

The following limitations apply to dynamic profiles for VPLS on MX Series routers:

- The **native-vlan-id** statement is not supported.
- The **native-inner-vlan-id** statement is not supported.
- The **interface-mode access** statement option is not supported.
- The **vlan-id-range** statement is not supported.



In many cases, a configuration using dynamic profiles is more efficient than a static configuration, as shown by the examples in this topic.

- [VPLS Pseudowire Interfaces Without Dynamic Profiles on page 621](#)
- [VPLS Pseudowire Interfaces and Dynamic Profiles on page 622](#)
- [CE Routers Without Dynamic Profiles on page 623](#)
- [CE Routers and Dynamic Profiles on page 624](#)

## VPLS Pseudowire Interfaces Without Dynamic Profiles

Consider the following configuration, which does not use dynamic profiles to manipulate VLAN identifiers:

```
[edit routing-instances]
green {
 instance-type vpls;
 interface ge-0/0/1.1;
 interface ge-0/0/2.1;
 interface ge-0/0/3.1;
 vlan-tags outer 200 inner 100;
 protocols vpls {
 vpls-id 10;
 neighbor 10.1.1.20;
 }
 {...more...}
}

[edit interfaces]
ge-0/0/1 {
 unit 0 {
 vlan-id 10;
 }
}
ge-0/0/2 {
 unit 0 {
 vlan-id 20;
 }
}
ge-0/0/3 {
 unit 0 {
 vlan-id 30;
 }
}
```



**NOTE:** This is not a complete router configuration.

With this configuration, broadcast packets inside frames arriving with VLAN identifier 10 on **ge-0/0/1** are normalized to a dual-tagged frame with an outer VLAN value of 200 and an inner VLAN value of 100. The broadcast packet and frames exiting **ge-0/0/2** or **ge-0/0/3** have the outer VLAN value stripped and the inner VLAN value swapped to 20 and 30 respectively, according to the interface configuration. However, this stripping of

the outer VLAN tag and the swapping is extra work, because the frames will still egress the VPLS pseudowire in routing instance **green** with an outer VLAN tag value of 200 and an inner VLAN tag value of 100, also according to the configuration.

The same configuration can be accomplished more effectively using dynamic profiles.

## VPLS Pseudowire Interfaces and Dynamic Profiles

Consider the following configuration, which uses dynamic profiles to manipulate VLAN identifiers:

```
[edit routing-instances]
green {
 instance-type vpls;
 interface ge-0/0/1.1;
 interface ge-0/0/2.1;
 interface ge-0/0/3.1;
 vlan-id 100; # Desired inner VLAN tag on the VPLS pseudowire
 protocols vpls {
 vpls-id 10;
 neighbor 10.1.1.20 {
 associate-profile green_vpls_pw_1; # The profile
 }
 }
 {...more...}
}

[edit interfaces]
ge-0/0/1 {
 unit 0 {
 vlan-id 10;
 }
}
ge-0/0/2 {
 unit 0 {
 vlan-id 20;
 }
}
ge-0/0/3 {
 unit 0 {
 vlan-id 30;
 }
}

[edit dynamic-profiles]
green_vpls_pw_1 interfaces $junos-interface-ifd-name {
 unit $junos-underlying-unit-number {
 vlan-tags outer 200 inner 100;
 }
}
```



**NOTE:** This is not a complete router configuration.

With this configuration, broadcast packets inside frames arriving with VLAN identifier 10 on **ge-0/0/1** are normalized to a frame with VLAN identifier 100. The broadcast packet and frames exiting **ge-0/0/2** or **ge-0/0/3** have this VLAN value swapped to 20 and 30 respectively, according to the interface configuration. Frames egress the VPLS pseudowire in routing instance **green** with an outer VLAN tag value of 200 pushed on top of the normalized value.

## CE Routers Without Dynamic Profiles

You can apply a dynamic profile to an entire VPLS configuration, not just a neighbor.

Consider the following configuration, which does not use dynamic profiles to manipulate VLAN identifiers on a customer edge (CE) router with VLAN identifier 100:

```
[edit routing-instances]
green {
 instance-type vpls;
 interface ge-0/0/1.1;
 interface ge-0/0/2.1;
 interface ge-0/0/3.1;
 vlan-tags outer 200 inner 100;
 protocols vpls {
 vpls-id 10;
 neighbor 10.1.1.20;
 }
 {...more...}
}

[edit interfaces]
ge-0/0/1 {
 unit 0 {
 vlan-id 100;
 }
}
ge-0/0/2 {
 unit 0 {
 vlan-id 100;
 }
}
ge-0/0/3 {
 unit 0 {
 vlan-id 100;
 }
}
```



**NOTE:** This is not a complete router configuration.

With this configuration, broadcast packets inside frames arriving on **ge-0/0/1** are normalized to a dual-tagged frame with an outer VLAN value of 200 and an inner VLAN value of 100. The same configuration can be accomplished using dynamic profiles.

## CE Routers and Dynamic Profiles

Consider the following configuration, which uses dynamic profiles at the **protocols** level:

```
[edit routing-instances]
green {
 instance-type vpls;
 interface ge-0/0/1.1;
 interface ge-0/0/2.1;
 interface ge-0/0/3.1;
 vlan-id 100; # Desired inner VLAN tag on the VPLS pseudowire
 protocols vpls {
 associate-profile green_vpls_pw_2; # The profile
 vpls-id 10;
 neighbor 10.1.1.20;
 }
 {...more...}
}

[edit interfaces]
ge-0/0/1 {
 unit 0 {
 vlan-id 100;
 }
}
ge-0/0/2 {
 unit 0 {
 vlan-id 100;
 }
}
ge-0/0/3 {
 unit 0 {
 vlan-id 100;
 }
}

[edit dynamic-profiles]
green_vpls_pw_2 interfaces $junos-interface-ifd-name {
 unit $junos-underlying-unit-number {
 vlan-tags outer 200 inner 100;
 }
}
```



**NOTE:** This is not a complete router configuration.

With this configuration, broadcast packets inside frames arriving with VLAN identifier 100 on **ge-0/0/1** are normalized to a frame with VLAN identifier 100 (in this case, they are unchanged). The broadcast packet and frames exiting **ge-0/0/2** or **ge-0/0/3** are unchanged as well, according to the interface configuration. Frames egress the VPLS pseudowire in routing instance **green** with an outer VLAN tag value of 200 pushed on top of the normalized value.

**Related Documentation**

- [Layer 2 VPNs and VPLS Feature Guide for Routing Devices](#)
- [Example: Configuring VPLS Pseudowires with Dynamic Profiles—Complex Solutions on page 625](#)

## Example: Configuring VPLS Pseudowires with Dynamic Profiles—Complex Solutions

Dynamic profiles for VPLS pseudowires can be helpful in a variety of VLAN configurations. This section explores some of these situations through examples.



**NOTE:** These examples are not complete router configurations.

All of the examples in this section address the same basic topology. A routing instance **blue** uses a trunk bridge to connect different departments in an organization, each with their own VLANs, at two different sites. The organization uses a BGP-based VPLS with a virtual switch to accomplish this.

- [Configuration of Routing Instance and Interfaces Without Dynamic Profiles on page 625](#)
- [Configuration of Routing Instance and Interfaces Using Dynamic Profiles on page 626](#)
- [Configuration of Tag Translation Using Dynamic Profiles on page 628](#)

### Configuration of Routing Instance and Interfaces Without Dynamic Profiles

The basic configuration of routing instance and interfaces without dynamic profiles follows:

```
[edit routing-instance blue]
instance-type virtual-switch;
route-distinguisher 10.1.1.10:1;
vrf-target target:1000:1;
interface ge-3/0/0; # The trunk interface
bridge-domains {
 sales {
 vlan-id 10;
 interface ge-0/0/0.1;
 ... # Other interfaces and statements for Sales
 }
 engineering {
 vlan-id 20;
 interface ge-1/0/2.0;
 ... # Other interfaces and statements for Engineering
 }
 accounting {
 vlan-id 30;
 interface ge-2/0/3.0;
 ... # Other interfaces and statements for Accounting
 }
 others {
 vlan-id-list [40 50]; # Other departments
 }
}
```

```

protocols vpls {
 site-range 10;
 site sample-site-1 {
 site-identifier 1;
 }
}
... # Other statements for instance Blue

[edit interfaces]
ge-0/0/1 {
 unit 0 {
 vlan-id 100;
 }
}
ge-3/0/0 {
 unit 0 {
 family bridge {
 interface-mode trunk; # This is the trunk
 vlan-id-list [10 20 30 40 50];
 }
 }
}
... # More interface statements

```

This configuration switches the departmental VLAN traffic (sales, engineering, etc.) bridge domains over the VPLS pseudowire trunk connecting to the other site.

## Configuration of Routing Instance and Interfaces Using Dynamic Profiles

Here is how dynamic profiles can be applied to this basic configuration.

First, consider the requirement to push an outer VLAN tag value of 200 onto the VPLS pseudowire frames on egress. Dynamic profiles easily satisfy this requirement.

```

[edit routing-instance green]
instance-type virtual-switch;
... # Other routing instance statements
protocols vpls {
 site-range 10;
 site sample-site-1 {
 site-identifier 1;
 }
 associate-profile green_vpls_pw_1; # Apply profile here
}
... # Other routing instance statements

[edit dynamic-profiles]
green_vpls_pw_1 interfaces $junos-interface-ifd-name {
 unit $junos-underlying-unit-number {
 vlan-id 200; # This is the outer tag
 family bridge {
 interface-mode trunk;
 inner-vlan-id-list [10 20 30 40 50];
 }
 }
}

```



**NOTE:** This is not a complete router configuration.

With the dynamic profile, a packet in a frame arriving on an interface is classified as belonging to one of the bridge domains (VLANs 10–50). At the egress of the trunk VPLS pseudowire, the outer VLAN tag 200 is pushed onto the frame. At the ingress of the pseudowire at the remote location, the outer VLAN tag 200 is removed and the frame is delivered to the appropriate bridge domain.

But what if the packets associated with the Accounting VLAN are not to be forwarding to the remote site? Dynamic profiles are useful here as well.

This configuration keeps the Accounting frames from reaching the remote site.

```
[edit routing-instances green]
instance-type virtual-switch;
... # Other routing instance statements
protocols vpls {
 site-range 10;
 site sample-site-1 {
 site-identifier 1;
 }
 associate-profile green_vpls_pw_2; # Apply profile here
}
... # Other routing instance statements

[edit dynamic-profiles]
green_vpls_pw_2 interfaces $junos-interface-ifd-name {
 unit $junos-underlying-unit-number {
 family bridge {
 interface-mode trunk;
 inner-vlan-id-list [10 20 40 50]; # Removed Accounting VLAN 30
 }
 }
}
}
```



**NOTE:** This is not a complete router configuration.

In this case, frames arriving on the interfaces are classified according to their bridge domains and switched, if necessary, to the VPLS pseudowire trunk, except for Engineering frames. Engineering frames (VLAN 30) are only switched within the interfaces listed within bridge domain **accounting** and any statically configured trunk interfaces and are prevented from crossing the VPLS pseudowire due to the absence of VLAN 30 on the trunk.

We can combine the two examples and use dynamic profiles to forward the frames (other than **accounting** frames) to the remote site with an out tag of 200.

This configuration keeps the Accounting frames from reaching the remote site and pushes an outer tag of 200 on VPLS pseudowire traffic.

```
[edit routing-instances green]
```

```

instance-type virtual-switch;
... # Other routing instance statements
protocols vpls {
 site-range 10;
 site sample-site-1 {
 site-identifier 1;
 }
 associate-profile green_vpls_pw_3; # Apply profile here
}
... # Other routing instance statements

[edit dynamic-profiles]
green_vpls_pw_3 interfaces $junos-interface-ifd-name {
 unit $junos-underlying-unit-number {
 vlan-id 200; # This is the outer tag
 family bridge {
 interface-mode trunk;
 inner-vlan-id-list [10 20 40 50]; # Removed Accounting VLAN 30
 }
 }
}

```



**NOTE:** This is not a complete router configuration.

In this case, frames arriving on the interfaces are classified according to their bridge domains and switched, if necessary, to the VPLS pseudowire trunk with an outer VLAN tag of 200, except for Engineering frames. Engineering frames (VLAN 30) are only switched within the interfaces listed within bridge domain **accounting** and any statically configured trunk interfaces and are prevented from crossing the VPLS pseudowire due to the absence of VLAN 30 on the trunk.

## Configuration of Tag Translation Using Dynamic Profiles

Consider a final case where the bridge domain VLANs need translation at the VPLS pseudowire trunk interface. In this case, **sales** (VLAN 10) is mapped to VLAN 110 and **engineering** (VLAN 20) is mapped to VLAN 120.

This configuration adds tag translation to the VPLS pseudowire traffic.

```

[edit routing-instances green]
instance-type virtual-switch;
... # Other routing instance statements
protocols vpls {
 site-range 10;
 site sample-site-1 {
 site-identifier 1;
 }
 associate-profile green_vpls_pw_4; # Apply profile here
}
... # Other routing instance statements

[edit dynamic-profiles]
green_vpls_pw_4 interfaces $junos-interface-ifd-name {

```



```

unit $junos-underlying-unit-number {
 family bridge {
 interface-mode trunk;
 vlan-id-list [10 20 30 40 50]; # All VLANs
 vlan-rewrite translate 110 10; # Sales VLAN
 vlan-rewrite translate 120 20; # Engineering VLAN
 }
}

```



**NOTE:** This is not a complete router configuration.

This translates the **sales** and **engineering** VLAN tags exiting the VPLS pseudowire accordingly. At the ingress of the VPLS pseudowire, VLANs 110 and 120 are translated back to 10 and 20, respectively.

**Related  
Documentation**

- *Layer 2 VPNs and VPLS Feature Guide for Routing Devices*
- [Example: Configuring VPLS Pseudowires with Dynamic Profiles—Basic Solutions on page 620](#)

## Configuring the FAT Flow Label for FEC 128 VPLS Pseudowires for Load-Balancing MPLS Traffic

This topic shows how to configure flow-aware transport of pseudowires (FAT) flow labels for forwarding equivalence class (FEC) 128 virtual private LAN service (VPLS) pseudowires for load-balancing MPLS traffic.

FAT flow labels enable load-balancing of MPLS packets across equal-cost multipath (ECMP) paths or link aggregation groups (LAGs) without the need for deep packet inspection of the payload. FAT flow labels can be used for LDP-signaled FEC 128 and FEC 129 pseudowires for VPLS and virtual private wire service (VPWS) networks.

You can configure FAT flow labels to be signaled by LDP on FEC 128 VPLS pseudowires by including the **flow-label-transmit** and **flow-label-receive** configuration statements at the **[edit routing-instances *instance-name* protocols vpls]** hierarchy level. This configuration sets the T bit and R bit advertisement to 1 (the default being 0) in the Sub-TLV field, which is one of the interface parameters of the FEC for the LDP label-mapping message header. This configuration is applicable for all the pseudowires providing full mesh connectivity from the VPLS routing instance to all its neighbors.

Before you begin:

1. Configure the device interfaces and enable MPLS on all the interfaces on the provider edge (PE) router.
2. Configure MPLS and an LSP from the ingress PE router to the remote egress PE router.
3. Configure an interior gateway protocol (IGP) on the PE router and provider (P) routers.

4. Configure the circuits between the PE routers and the customer edge (CE) routers.
5. Configure LDP on all the interfaces.

To configure the FAT flow label for an FEC 128 VPLS pseudowire, on the ingress PE router:

1. Configure the FEC 128 VPLS routing instance.

```
[edit]
user@PE1# set routing-instances instance-name instance-type vpls
user@PE1# set routing-instances instance-name interface interface-name
user@PE1# set routing-instances instance-name protocols vpls vpls-id vpls-id
user@PE1# set routing-instances instance-name protocols vpls neighbor neighbor-id
user@PE1# set routing-instances instance-name protocols vpls neighbor neighbor-id
```

2. Configure the routing instance to signal the capability to push the flow label in the transmit direction to the remote PE router.

```
[edit routing-instances instance-name protocols vpls]
user@PE1# set flow-label-transmit
```

3. Configure the routing instance to signal the capability to pop the flow label in the receive direction to the remote PE router.

```
[edit routing-instances instance-name protocols vpls]
user@PE1# set flow-label-receive
```

4. Verify and commit the configuration.

For example:

```
[edit routing-instances]
user@PE1# show
ldp-fec128-signaled-vpls {
 instance-type vpls;
 interface ge-0/0/1.0;
 protocols {
 vpls {
 vpls-id 100;
 flow-label-transmit;
 flow-label-receive;
 }
 }
}
```

5. Repeat the configuration on the remote egress PE router.

**Related  
Documentation**

- [Configuring the FAT Flow Label for FEC 128 VPWS Pseudowires for Load-Balancing MPLS Traffic on page 534](#)
- [Configuring the FAT Flow Label for FEC 129 VPWS Pseudowires for Load-Balancing MPLS Traffic on page 536](#)
- [Configuring the FAT Flow Label for FEC 129 VPLS Pseudowires for Load-Balancing MPLS Traffic on page 631](#)
- [FAT Flow Labels Overview](#)

## Configuring the FAT Flow Label for FEC 129 VPLS Pseudowires for Load-Balancing MPLS Traffic

This topic shows how to configure flow-aware transport of pseudowires (FAT) flow labels for forwarding equivalence class (FEC) 129 virtual private LAN service (VPLS) pseudowires for load-balancing MPLS traffic.

FAT flow labels enable load-balancing of MPLS packets across equal-cost multipath (ECMP) paths or link aggregation groups (LAGs) without the need for deep packet inspection of the payload. FAT flow labels can be used for LDP-signaled FEC 128 and FEC 129 pseudowires for VPLS and virtual private wire service (VPWS) networks.

You can configure FAT flow labels to be signaled by LDP on FEC 129 VPLS pseudowires by including the **flow-label-transmit** and **flow-label-receive** configuration statements at the **[edit routing-instances *instance-name* protocols vpls]** hierarchy level. This configuration sets the T bit and R bit advertisement to 1 (the default being 0) in the Sub-TLV field, which is part one of the interface parameters of the FEC for the LDP label-mapping message header. This configuration is applicable for all the pseudowires providing full mesh connectivity from the VPLS routing instance to all its neighbors.

Before you begin:

1. Configure the device interfaces and enable MPLS on all the interfaces.
2. Configure MPLS and an LSP from the ingress provider edge (PE) router to the remote PE router.
3. Configure IBGP sessions between the PE routers.
4. Configure an interior gateway protocol (IGP) on the PE router and provider (P) routers.
5. Configure the circuits between the PE routers and the customer edge (CE) routers.
6. Configure LDP on all the interfaces.

To configure the FAT flow label for an FEC 129 VPLS pseudowire, on the ingress PE router:

1. Configure the FEC 129 VPLS routing instance.

```
[edit]
user@PE1# set routing-instances instance-name instance-type vpls
user@PE1# set routing-instances instance-name interface interface-name
user@PE1# set routing-instances instance-name route-distinguisher (as-number:id |
ip-address:id)
user@PE1# set routing-instances instance-name l2vpn-id (as-number:x:y | ip-address:id)
user@PE1# set routing-instances instance-name vrf-target target:x:y
```

2. Configure the routing instance to signal the capability to push the flow label in the transmit direction to the remote PE router.

```
[edit routing-instances instance-name protocols vpls]
user@PE1# set flow-label-transmit
```

3. Configure the routing instance to signal the capability to pop the flow label in the receive direction to the remote PE router.

```
[edit routing-instances instance-name protocols vpls]
user@PE1# set flow-label-receive
```

4. Verify and commit the configuration.

For example:

```
[edit routing-instances]
user@PE1# show
ldp-fec129-signaled-vpls {
 instance-type vpls;
 interface fe-0/0/0.0;
 route-distinguisher 10.255.245.45:100;
 l2vpn-id l2vpn-id:100:100;
 vrf-target target:100:100;
 protocols {
 vpls {
 flow-label-transmit;
 flow-label-receive;
 }
 }
}
```

5. Repeat the configuration on the remote egress PE router.

#### Related Documentation

- [Configuring the FAT Flow Label for FEC 128 VPWS Pseudowires for Load-Balancing MPLS Traffic on page 534](#)
- [Configuring the FAT Flow Label for FEC 128 VPLS Pseudowires for Load-Balancing MPLS Traffic on page 629](#)
- [Configuring the FAT Flow Label for FEC 129 VPWS Pseudowires for Load-Balancing MPLS Traffic on page 536](#)
- [FAT Flow Labels Overview](#)

## Example: Configuring H-VPLS BGP-Based and LDP-Based VPLS Interoperation

This example shows how to configure the hierarchical virtual private LAN service (H-VPLS) in a scenario that uses both LDP-based VPLS and BGP-based VPLS interoperating in a multihoming deployment. This scenario is useful when a customer deployment has the two different types of VPLS in use, and you need to integrate them. Another example is when ISP-A is running BGP-based VPLS and ISP-B is running the LDP-based VPLS, and the two ISPs are merging their networks.

### Requirements

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

### Overview

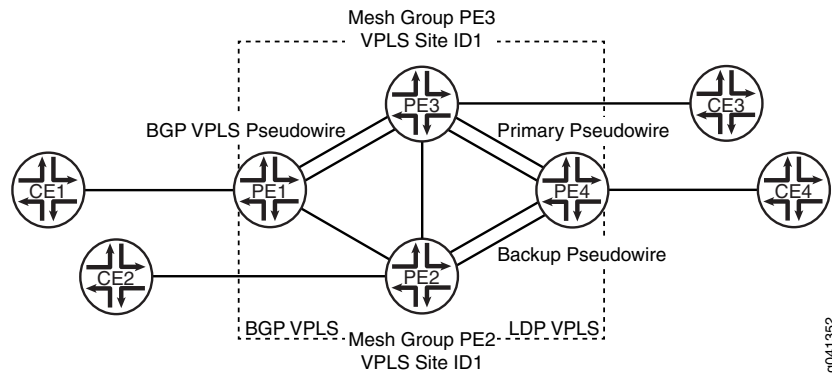
In this example, Device PE2 and Device PE3 are acting as internetworking provider edge (PE) routers with BGP-based as well as LDP-based VPLS termination.

The devices in this example have the following roles:

- BGP VPLS only PE—Device PE1
- LDP VPLS only PE—Device PE4
- BGP-LDP VPLS PE—Device PE2 and Device PE3

Figure 54 on page 633 shows the topology used in this example.

Figure 54: H-VPLS with LDP-Based and BGP-Based VPLS Interoperation



From Device PE4, the pseudowire to Device PE3 is the primary or working path. The pseudowire Device PE2 is the backup path.

“CLI Quick Configuration” on page 633 shows the configuration for all of the devices in Figure 54 on page 633. The section “Step-by-Step Procedure” on page 636 describes the steps on Device PE1, Device PE2, and Device PE4.

## 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 PE1
set interfaces ge-2/0/5 encapsulation ethernet-vpls
set interfaces ge-2/0/5 unit 0 description to_CE1
set interfaces ge-2/0/5 unit 0 family vpls
set interfaces fe-2/0/9 unit 0 description to_PE2
set interfaces fe-2/0/9 unit 0 family inet address 10.10.3.1/30
set interfaces fe-2/0/9 unit 0 family mpls
set interfaces fe-2/0/10 unit 0 description to_PE3
set interfaces fe-2/0/10 unit 0 family inet address 10.10.1.1/30
set interfaces fe-2/0/10 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 192.0.2.1/24
set protocols mpls interface fe-2/0/10.0
set protocols mpls interface fe-2/0/9.0
set protocols ldp interface fe-2/0/10.0
set protocols ldp interface fe-2/0/9.0
set protocols ldp interface lo0.0
set protocols bgp group internal-peers type internal
set protocols bgp group internal-peers local-address 192.0.2.1
```

```

set protocols bgp group internal-peers family l2vpn signaling
set protocols bgp group internal-peers neighbor 192.0.2.2
set protocols bgp group internal-peers neighbor 192.0.2.3
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface fe-2/0/10.0
set protocols ospf area 0.0.0.0 interface fe-2/0/9.0
set routing-instances h-vpls-PE1 instance-type vpls
set routing-instances h-vpls-PE1 interface ge-2/0/5.0
set routing-instances h-vpls-PE1 route-distinguisher 1:1
set routing-instances h-vpls-PE1 vrf-target target:1:1
set routing-instances h-vpls-PE1 protocols vpls interface ge-2/0/5.0
set routing-instances h-vpls-PE1 protocols vpls site PE1-vpls site-identifier 2
set routing-options autonomous-system 64510

```

**Device PE2**

```

set interfaces ge-2/0/6 encapsulation ethernet-vpls
set interfaces ge-2/0/6 unit 0 description to_CE2
set interfaces ge-2/0/6 unit 0 family vpls
set interfaces fe-2/0/8 unit 0 description to_PE3
set interfaces fe-2/0/8 unit 0 family inet address 10.10.4.2/30
set interfaces fe-2/0/8 unit 0 family mpls
set interfaces fe-2/0/9 unit 0 description to_PE4
set interfaces fe-2/0/9 unit 0 family inet address 10.10.5.1/30
set interfaces fe-2/0/9 unit 0 family mpls
set interfaces fe-2/0/10 unit 0 description to_PE1
set interfaces fe-2/0/10 unit 0 family inet address 10.10.3.2/30
set interfaces fe-2/0/10 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 192.0.2.2/24
set protocols mpls interface fe-2/0/10.0
set protocols mpls interface fe-2/0/9.0
set protocols mpls interface fe-2/0/8.0
set protocols ldp interface fe-2/0/10.0
set protocols ldp interface fe-2/0/9.0
set protocols ldp interface fe-2/0/8.0
set protocols ldp interface lo0.0
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 192.0.2.2
set protocols bgp group ibgp family l2vpn signaling
set protocols bgp group ibgp neighbor 192.0.2.3
set protocols bgp group ibgp neighbor 192.0.2.1
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface fe-2/0/10.0
set protocols ospf area 0.0.0.0 interface fe-2/0/9.0
set protocols ospf area 0.0.0.0 interface fe-2/0/8.0
set routing-instances h-vpls-PE2 instance-type vpls
set routing-instances h-vpls-PE2 interface ge-2/0/6.0
set routing-instances h-vpls-PE2 route-distinguisher 1:2
set routing-instances h-vpls-PE2 vrf-target target:1:1
set routing-instances h-vpls-PE2 protocols vpls interface ge-2/0/6.0
set routing-instances h-vpls-PE2 protocols vpls site PE2-vpls site-identifier 1
set routing-instances h-vpls-PE2 protocols vpls site PE2-vpls multi-homing
set routing-instances h-vpls-PE2 protocols vpls site PE2-vpls mesh-group h-vpls-PE2
set routing-instances h-vpls-PE2 protocols vpls vpls-id 100
set routing-instances h-vpls-PE2 protocols vpls mesh-group h-vpls-PE2 vpls-id 100
set routing-instances h-vpls-PE2 protocols vpls mesh-group h-vpls-PE2 local-switching
set routing-instances h-vpls-PE2 protocols vpls mesh-group h-vpls-PE2 neighbor 192.0.2.4
set routing-options autonomous-system 64510

```

```

Device PE3 set interfaces fe-2/0/8 unit 0 description to_PE2
 set interfaces fe-2/0/8 unit 0 family inet address 10.10.4.1/30
 set interfaces fe-2/0/8 unit 0 family mpls
 set interfaces fe-2/0/9 unit 0 description to_PE4
 set interfaces fe-2/0/9 unit 0 family inet address 10.10.6.1/30
 set interfaces fe-2/0/9 unit 0 family mpls
 set interfaces fe-2/0/10 unit 0 description to_PE1
 set interfaces fe-2/0/10 unit 0 family inet address 10.10.1.2/30
 set interfaces fe-2/0/10 unit 0 family mpls
 set interfaces ge-2/1/3 encapsulation ethernet-vpls
 set interfaces ge-2/1/3 unit 0 description to_CE3
 set interfaces ge-2/1/3 unit 0 family vpls
 set interfaces lo0 unit 0 family inet address 192.0.2.3/24
 set protocols mpls interface fe-2/0/10.0
 set protocols mpls interface fe-2/0/8.0
 set protocols mpls interface fe-2/0/9.0
 set protocols ldp interface fe-2/0/10.0
 set protocols ldp interface fe-2/0/9.0
 set protocols ldp interface fe-2/0/8.0
 set protocols ldp interface lo0.0
 set protocols bgp group internal-peers type internal
 set protocols bgp group internal-peers local-address 192.0.2.3
 set protocols bgp group internal-peers family l2vpn signaling
 set protocols bgp group internal-peers neighbor 192.0.2.2
 set protocols bgp group internal-peers neighbor 192.0.2.1
 set protocols ospf traffic-engineering
 set protocols ospf area 0.0.0.0 interface lo0.0 passive
 set protocols ospf area 0.0.0.0 interface fe-2/0/10.0
 set protocols ospf area 0.0.0.0 interface fe-2/0/8.0
 set protocols ospf area 0.0.0.0 interface fe-2/0/9.0
 set routing-instances h-vpls-PE3 instance-type vpls
 set routing-instances h-vpls-PE3 interface ge-2/1/3.0
 set routing-instances h-vpls-PE3 route-distinguisher 1:3
 set routing-instances h-vpls-PE3 vrf-target target:1:1
 set routing-instances h-vpls-PE3 protocols vpls interface ge-2/1/3.0
 set routing-instances h-vpls-PE3 protocols vpls site PE3-vpls site-identifier 1
 set routing-instances h-vpls-PE3 protocols vpls site PE3-vpls multi-homing
 set routing-instances h-vpls-PE3 protocols vpls site PE3-vpls mesh-group h-vpls-PE3
 set routing-instances h-vpls-PE3 protocols vpls vpls-id 100
 set routing-instances h-vpls-PE3 protocols vpls mesh-group h-vpls-PE3 vpls-id 100
 set routing-instances h-vpls-PE3 protocols vpls mesh-group h-vpls-PE3 local-switching
 set routing-instances h-vpls-PE3 protocols vpls mesh-group h-vpls-PE3 neighbor 192.0.2.4
 set routing-options autonomous-system 64510

Device PE4 set interfaces fe-2/0/9 unit 0 description to_PE3
 set interfaces fe-2/0/9 unit 0 family inet address 10.10.6.2/30
 set interfaces fe-2/0/9 unit 0 family mpls
 set interfaces fe-2/0/10 unit 0 description to_PE2
 set interfaces fe-2/0/10 unit 0 family inet address 10.10.5.2/30
 set interfaces fe-2/0/10 unit 0 family mpls
 set interfaces ge-2/1/7 encapsulation ethernet-vpls
 set interfaces ge-2/1/7 unit 0 description to_CE4
 set interfaces ge-2/1/7 unit 0 family vpls
 set interfaces lo0 unit 0 family inet address 192.0.2.4/24
 set protocols mpls interface fe-2/0/10.0

```

```

set protocols mpls interface fe-2/0/9.0
set protocols ldp interface fe-2/0/10.0
set protocols ldp interface fe-2/0/9.0
set protocols ldp interface lo0.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface fe-2/0/10.0
set protocols ospf area 0.0.0.0 interface fe-2/0/9.0
set routing-instances ldp-vpls instance-type vpls
set routing-instances ldp-vpls interface ge-2/1/7.0
set routing-instances ldp-vpls protocols vpls vpls-id 100
set routing-instances ldp-vpls protocols vpls neighbor 192.0.2.3
set routing-instances ldp-vpls protocols vpls neighbor 192.0.2.2

```

**Device CE1**

```

set interfaces ge-2/0/8 unit 0 description to_PE1
set interfaces ge-2/0/8 unit 0 family inet address 172.16.0.1/24
set interfaces lo0 unit 0 family inet address 10.255.14.214/32
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-2/0/8.0

```

**Device CE2**

```

set interfaces ge-2/1/5 unit 0 description to_PE2
set interfaces ge-2/1/5 unit 0 family inet address 172.16.0.2/24
set interfaces lo0 unit 0 family inet address 10.255.14.215/32
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-2/1/5.0

```

**Device CE3**

```

set interfaces ge-2/0/9 unit 0 description to_PE3
set interfaces ge-2/0/9 unit 0 family inet address 172.16.0.3/24
set interfaces lo0 unit 0 family inet address 10.255.14.218/32
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-2/0/9.0

```

**Device CE4**

```

set interfaces ge-2/1/6 unit 0 description to_PE4
set interfaces ge-2/1/6 unit 0 family inet address 172.16.0.4/24
set interfaces lo0 unit 0 family inet address 10.255.14.219/32
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-2/1/6.0

```

**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 BGP-based VPLS PE device:

1. Configure the interfaces.

On the device interface that connects to the customer edge, enable VPLS encapsulation and the VPLS address family.

On the core-facing interfaces, enable MPLS labels.

```

[edit interfaces]
user@PE1# set ge-2/0/5 encapsulation ethernet-vpls
user@PE1# set ge-2/0/5 unit 0 description to_CE1
user@PE1# set ge-2/0/5 unit 0 family vpls

```



```

user@PE1# set fe-2/0/10 unit 0 description to_PE3
user@PE1# set fe-2/0/10 unit 0 family inet address 10.10.1.1/30
user@PE1# set fe-2/0/10 unit 0 family mpls

```

```

user@PE1# set fe-2/0/9 unit 0 description to_PE2
user@PE1# set fe-2/0/9 unit 0 family inet address 10.10.3.1/30
user@PE1# set fe-2/0/9 unit 0 family mpls

```

```

user@PE1# set lo0 unit 0 family inet address 192.0.2.1/24

```

2. Enable MPLS and LDP on the interfaces.

On the MTU device interfaces that connect to other PE devices, configure MPLS and LDP.

```

[edit protocols mpls]
user@PE1# set interface fe-2/0/10.0
user@PE1# set interface fe-2/0/9.0

```

```

[edit protocols ldp]
user@PE1# set interface fe-2/0/10.0
user@PE1# set interface fe-2/0/9.0
user@PE1# set interface lo0.0

```

3. Enable routing on the interfaces.

On the MTU device interfaces that connect to other PE devices, configure an interior gateway protocol (IGP), such as OSPF or IS-IS.

```

[edit protocols ospf area 0.0.0.0]
user@PE1# set interface lo0.0 passive
user@PE1# set interface fe-2/0/10.0
user@PE1# set interface fe-2/0/9.0

```

4. Configure BGP with Layer 2 VPN signaling.

The **l2vpn signaling** statement enables support for both VPLS and Layer 2 VPN advertisement under the same network layer reachability information (NLRI).

The internal IBGP (IBGP) full mesh includes Device PE1, Device PE2, and Device PE3. Device PE4 is not included.

```

[edit protocols bgp group internal-peers]
user@PE1# set type internal
user@PE1# set local-address 192.0.2.1
user@PE1# set family l2vpn signaling
user@PE1# set neighbor 192.0.2.2
user@PE1# set neighbor 192.0.2.3

```

5. Configure the VPLS routing instance.

Because this is BGP-based VPLS, include a route distinguisher, a VRF target, and a site name and ID.

```

[edit routing-instances h-vpls-PE1]
user@PE1# set instance-type vpls
user@PE1# set interface ge-2/0/5.0
user@PE1# set route-distinguisher 1:1

```

```
user@PE1# set vrf-target target:1:1
```

```
[edit routing-instances h-vpls-PE1 protocols vpls]
```

```
user@PE1# set interface ge-2/0/5.0
```

```
user@PE1# set site PE1-vpls site-identifier 2
```

6. Configure the autonomous system (AS) number.

```
[edit routing-options]
```

```
user@PE1# set autonomous-system 64510
```

### 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 BGP-LDP-based VPLS PE device:

1. Configure the interfaces.

On the PE-r device interface that connects to the customer edge, configure one of the VPLS encapsulation types and the VPLS address family. This enables VPLS.

On the core-facing interfaces, enable MPLS labels.

```
[edit interfaces]
```

```
user@PE2# set ge-2/0/6 encapsulation ethernet-vpls
```

```
user@PE2# set ge-2/0/6 unit 0 description to_CE2
```

```
user@PE2# set ge-2/0/6 unit 0 family vpls
```

```
user@PE2# set fe-2/0/10 unit 0 description to_PE1
```

```
user@PE2# set fe-2/0/10 unit 0 family inet address 10.10.3.2/30
```

```
user@PE2# set fe-2/0/10 unit 0 family mpls
```

```
user@PE2# set fe-2/0/9 unit 0 description to_PE4
```

```
user@PE2# set fe-2/0/9 unit 0 family inet address 10.10.5.1/30
```

```
user@PE2# set fe-2/0/9 unit 0 family mpls
```

```
user@PE2# set fe-2/0/8 unit 0 description to_PE3
```

```
user@PE2# set fe-2/0/8 unit 0 family inet address 10.10.4.2/30
```

```
user@PE2# set fe-2/0/8 unit 0 family mpls
```

```
user@PE2# set lo0 unit 0 family inet address 192.0.2.2/24
```

2. Enable MPLS and LDP on the interfaces.

On the MTU device interfaces that connect to other PE devices, configure MPLS and LDP.

```
[edit protocols mpls]
```

```
user@PE2# set interface fe-2/0/10.0
```

```
user@PE2# set interface fe-2/0/9.0
```

```
user@PE2# set interface fe-2/0/8.0
```

```
[edit protocols ldp]
```

```
user@PE2# set interface fe-2/0/10.0
```

```

user@PE2# set interface fe-2/0/9.0
user@PE2# set interface fe-2/0/8.0
user@PE2# set interface lo0.0

```

3. Enable routing on the interfaces.

On the MTU device interfaces that connect to other PE devices, configure an interior gateway protocol (IGP), such as OSPF or IS-IS.

```

[edit protocols ospf area 0.0.0.0]
user@PE2# set interface lo0.0 passive
user@PE2# set interface fe-2/0/10.0
user@PE2# set interface fe-2/0/9.0
user@PE2# set interface fe-2/0/8.0

```

4. 

```
[edit protocols bgp group ibgp]
user@PE2# set type internal
user@PE2# set local-address 192.0.2.2
user@PE2# set family l2vpn signaling
user@PE2# set neighbor 192.0.2.3
user@PE2# set neighbor 192.0.2.1
```

5. Configure VPLS.

The **vpls-id** statement enables LDP signaling for the VPLS instance.

```

[edit routing-instances h-vpls-PE2]
user@PE2# set instance-type vpls
user@PE2# set interface ge-2/0/6.0
user@PE2# set route-distinguisher 1:2
user@PE2# set vrf-target target:1:1

```

```

[edit routing-instances h-vpls-PE2 protocols vpls]
user@PE2# set interface ge-2/0/6.0
user@PE2# set site PE2-vpls site-identifier 1
user@PE2# set site PE2-vpls multi-homing
user@PE2# set site PE2-vpls mesh-group h-vpls-PE2
user@PE2# set vpls-id 100
user@PE2# set mesh-group h-vpls-PE2 vpls-id 100
user@PE2# set mesh-group h-vpls-PE2 local-switching
user@PE2# set mesh-group h-vpls-PE2 neighbor 192.0.2.4

```

6. 

```
[edit routing-options]
user@PE2# set autonomous-system 64510
```

**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 LDP-based VPLS PE device:

1. Configure the interfaces.

On the PE-r device interface that connects to the customer edge, configure one of the VPLS encapsulation types and the VPLS address family. This enables VPLS.

On the core-facing interfaces, enable MPLS labels.

```
[edit interfaces]
user@PE4# set fe-2/0/10 unit 0 description to_PE2
user@PE4# set fe-2/0/10 unit 0 family inet address 10.10.5.2/30
user@PE4# set fe-2/0/10 unit 0 family mpls

user@PE4# set fe-2/0/9 unit 0 description to_PE3
user@PE4# set fe-2/0/9 unit 0 family inet address 10.10.6.2/30
user@PE4# set fe-2/0/9 unit 0 family mpls

user@PE4# set ge-2/1/7 encapsulation ethernet-vpls
user@PE4# set ge-2/1/7 unit 0 description to_CE4
user@PE4# set ge-2/1/7 unit 0 family vpls

user@PE4# set lo0 unit 0 family inet address 192.0.2.4/24
```

2. Enable MPLS and LDP on the interfaces.

On the MTU device interfaces that connect to other PE devices, configure MPLS and LDP.

```
[edit protocols mpls]
user@PE4# set interface fe-2/0/10.0
user@PE4# set interface fe-2/0/9.0
```

```
[edit protocols ldp]
user@PE4# set interface fe-2/0/10.0
user@PE4# set interface fe-2/0/9.0
user@PE4# set interface lo0.0
```

3. Enable routing on the interfaces.

On the MTU device interfaces that connect to other PE devices, configure an interior gateway protocol (IGP), such as OSPF or IS-IS.

```
[edit protocols ospf area 0.0.0.0]
user@PE4# set interface lo0.0 passive
user@PE4# set interface fe-2/0/10.0
user@PE4# set interface fe-2/0/9.0
```

4. Configure VPLS.

The **vpls-id** statement enables LDP signaling for the VPLS instance.

```
[edit routing-instances ldp-vpls]
user@PE4# set instance-type vpls
user@PE4# set interface ge-2/1/7.0
user@PE4# set protocols vpls vpls-id 100
```

```
[edit routing-instances ldp-vpls protocols vpls]
user@PE4# set neighbor 192.0.2.3
user@PE4# set neighbor 192.0.2.2
```

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

```

Device PE1 user@PE1# show interfaces
ge-2/0/5 {
 encapsulation ethernet-vpls;
 unit 0 {
 description to_CE1;
 family vpls;
 }
}
fe-2/0/9 {
}
unit 0 {
 description to_PE2;
 family inet {
 address 10.10.3.1/30;
 }
 family mpls;
}
}
fe-2/0/10 {
 unit 0 {
 description to_PE3;
 family inet {
 address 10.10.1.1/30;
 }
 family mpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.1/24;
 }
 }
}

user@PE1# show protocols
mpls {
 interface fe-2/0/10.0;
 interface fe-2/0/9.0;
}
bgp {
 group internal-peers {
 type internal;
 local-address 192.0.2.1;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.2;
 neighbor 192.0.2.3;
 }
}
ospf {
 area 0.0.0.0 {
 interface lo0.0 {
 passive;
 }
 }
}

```

```

 }
 interface fe-2/0/10.0;
 interface fe-2/0/9.0;
 }
}
ldp {
 interface fe-2/0/10.0;
 interface fe-2/0/9.0;
 interface lo0.0;
}

user@PE1# show routing-instances
h-vpls-PE1 {
 instance-type vpls;
 interface ge-2/0/5.0;
 route-distinguisher 1:1;
 vrf-target target:1:1;
 protocols {
 vpls {
 interface ge-2/0/5.0;
 site PE1-vpls {
 site-identifier 2;
 }
 }
 }
}

user@PE1# show routing-options
autonomous-system 64510;

```

**Device PE2**

```

user@PE2# show interfaces
ge-2/0/6 {
 encapsulation ethernet-vpls;
 unit 0 {
 description to_CE2;
 family vpls;
 }
}
fe-2/0/8 {
 unit 0 {
 description to_PE3;
 family inet {
 address 10.10.4.2/30;
 }
 family mpls;
 }
}
fe-2/0/9 {
 unit 0 {
 description to_PE4;
 family inet {
 address 10.10.5.1/30;
 }
 family mpls;
 }
}
fe-2/0/10 {

```

```

 unit 0 {
 description to_PE1;
 family inet {
 address 10.10.3.2/30;
 }
 family mpls;
 }
 }
 lo0 {
 unit 0 {
 family inet {
 address 192.0.2.2/24;
 }
 }
 }
}

user@PE2# show protocols
mpls {
 interface fe-2/0/10.0;
 interface fe-2/0/9.0;
 interface fe-2/0/8.0;
}
bgp {
 group ibgp {
 type internal;
 local-address 192.0.2.2;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.3;
 neighbor 192.0.2.1;
 }
}
ospf {
 area 0.0.0.0 {
 interface lo0.0 {
 passive;
 }
 interface fe-2/0/10.0;
 interface fe-2/0/9.0;
 interface fe-2/0/8.0;
 }
}
ldp {
 interface fe-2/0/10.0;
 interface fe-2/0/9.0;
 interface fe-2/0/8.0;
 interface lo0.0;
}

user@PE2# show routing-instances
h-vpls-PE2 {
 instance-type vpls;
 interface ge-2/0/6.0;
 route-distinguisher 1:2;
 vrf-target target:1:1;
}

```

```

protocols {
 vpls {
 interface ge-2/0/6.0;
 site PE2-vpls {
 site-identifier 1;
 multi-homing;
 mesh-group h-vpls-PE2;
 }
 vpls-id 100;
 mesh-group h-vpls-PE2 {
 vpls-id 100;
 local-switching;
 neighbor 192.0.2.4;
 }
 }
}

```

```

user@PE2# show routing-options
autonomous-system 64510;

```

**Device PE4**

```

user@PE4# show interfaces
ge-2/1/7 {
 encapsulation ethernet-vpls;
 unit 0 {
 description to_CE4;
 family vpls;
 }
}
fe-2/0/9 {
 unit 0 {
 description to_PE3;
 family inet {
 address 10.10.6.2/30;
 }
 family mpls;
 }
}
fe-2/0/10 {
 unit 0 {
 description to_PE2;
 family inet {
 address 10.10.5.2/30;
 }
 family mpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.4/24;
 }
 }
}

```

```

user@PE4# show protocols

```



```

mpls {
 interface fe-2/0/9.0;
 interface fe-2/0/10.0;
}
ospf {
 area 0.0.0.0 {
 interface lo0.0 {
 passive;
 }
 interface fe-2/0/9.0;
 interface fe-2/0/10.0;
 }
}
ldp {
 interface fe-2/0/10.0;
 interface fe-2/0/9.0;
 interface lo0.0;
}

user@PE4# show routing-instances
ldp-vpls {
 instance-type vpls;
 interface ge-2/1/7.0;
 protocols {
 vpls {
 vpls-id 100;
 neighbor 192.0.2.3;
 neighbor 192.0.2.2;
 }
 }
}

```

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

## Verification

Confirm that the configuration is working properly. In a multihoming scenario with BGP-LDP VPLS, the LDP pseudowires are in the down state for the backup PE (Device PE2). Whereas on the LDP-only VPLS PE (Device PE4), the pseudowires to the primary and backup BGP-LDP PE devices are in the up state.

- [Verifying the VPLS Connections on page 645](#)
- [Manually Triggering a Switch from the Active Pseudowire to the Backup Pseudowire on page 649](#)
- [Checking Connectivity on page 652](#)
- [Checking the BGP Layer 2 VPN Routing Tables on page 652](#)
- [Checking the Layer 2 Circuit Routing Tables on page 652](#)

### Verifying the VPLS Connections

**Purpose** Verify that the VPLS connections are working as expected.

**Action** From operational mode, enter the **show vpls connections** command.

```
user@PE1> show vpls connections
```

Layer-2 VPN connections:

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -> -- only outbound connection is up           |
| CN -- circuit not provisioned    | <- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unknown connection status  | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not available              |
| BK -- Backup connection          | ST -- Standby connection                       |
| PF -- Profile parse failure      | PB -- Profile busy                             |
| RS -- remote site standby        | SN -- Static Neighbor                          |
| LB -- Local site not best-site   | RB -- Remote site not best-site                |
| VM -- VLAN ID mismatch           |                                                |

Legend for interface status

Up -- operational

Dn -- down

Instance: h-vpls-PE1

Local site: PE1-vpls (2)

| connection-site                                                      | Type | St        | Time last up         | # Up trans |
|----------------------------------------------------------------------|------|-----------|----------------------|------------|
| 1                                                                    | rmt  | <b>Up</b> | Oct 16 16:52:27 2012 | 1          |
| Remote PE: 192.0.2.2, Negotiated control-word: No                    |      |           |                      |            |
| Incoming label: 800016, Outgoing label: 800009                       |      |           |                      |            |
| Local interface: vt-2/0/10.51380738, Status: Up, Encapsulation: VPLS |      |           |                      |            |
| Description: Intf - vpls h-vpls-PE1 local site 2 remote site 1       |      |           |                      |            |

```
user@PE2> show vpls connections
```

Layer-2 VPN connections:

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -> -- only outbound connection is up           |
| CN -- circuit not provisioned    | <- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unknown connection status  | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not available              |
| BK -- Backup connection          | ST -- Standby connection                       |
| PF -- Profile parse failure      | PB -- Profile busy                             |
| RS -- remote site standby        | SN -- Static Neighbor                          |
| LB -- Local site not best-site   | RB -- Remote site not best-site                |
| VM -- VLAN ID mismatch           |                                                |

## Legend for interface status

Up -- operational

Dn -- down

Instance: h-vpls-PE2

**BGP-VPLS State**

Local site: PE2-vpls (1)

| connection-site | Type | St | Time last up         | # Up trans |
|-----------------|------|----|----------------------|------------|
| 1               | rmt  | RN |                      |            |
| 2               | rmt  | Up | Oct 16 17:12:31 2012 | 1          |

Remote PE: 192.0.2.1, Negotiated control-word: No

Incoming label: 800257, Outgoing label: 800000

Local interface: vt-2/0/10.118489089, Status: Up, Encapsulation: VPLS

Description: Intf - vpls h-vpls-PE2 local site 1 remote site 2

**LDP-VPLS State**

VPLS-id: 100

Mesh-group connections: h-vpls-PE2

| Neighbor               | Type | St | Time last up         | # Up trans |
|------------------------|------|----|----------------------|------------|
| 192.0.2.4(vpls-id 100) | rmt  | Up | Oct 16 17:12:30 2012 | 1          |

Remote PE: 192.0.2.4, Negotiated control-word: No

Incoming label: 800000, Outgoing label: 800001

Negotiated PW status TLV: No

Local interface: vt-2/0/10.118489088, Status: Up, Encapsulation: ETHERNET

Description: Intf - vpls h-vpls-PE2 neighbor 192.0.2.4 vpls-id 100

user@PE3&gt; show vpls connections

Layer-2 VPN connections:

## Legend for connection status (St)

EI -- encapsulation invalid NC -- interface encapsulation not CCC/TCC/VPLS

EM -- encapsulation mismatch WE -- interface and instance encaps not same

VC-Dn -- Virtual circuit down NP -- interface hardware not present

CM -- control-word mismatch -&gt; -- only outbound connection is up

CN -- circuit not provisioned &lt;- -- only inbound connection is up

OR -- out of range Up -- operational

OL -- no outgoing label Dn -- down

LD -- local site signaled down CF -- call admission control failure

RD -- remote site signaled down SC -- local and remote site ID collision

LN -- local site not designated LM -- local site ID not minimum designated

RN -- remote site not designated RM -- remote site ID not minimum designated

XX -- unknown connection status IL -- no incoming label

MM -- MTU mismatch MI -- Mesh-Group ID not available

BK -- Backup connection ST -- Standby connection

PF -- Profile parse failure PB -- Profile busy

RS -- remote site standby SN -- Static Neighbor

LB -- Local site not best-site RB -- Remote site not best-site

VM -- VLAN ID mismatch

## Legend for interface status

Up -- operational

Dn -- down

Instance: h-vpls-PE3

**BGP-VPLS State**

Local site: PE3-vpls (1)

| connection-site | Type | St | Time last up | # Up trans |
|-----------------|------|----|--------------|------------|
| 1               | rmt  | LN |              |            |
| 2               | rmt  | LN |              |            |

**LDP-VPLS State**

VPLS-id: 100

Mesh-group connections: h-vpls-PE3

```

Neighbor Type St Time last up # Up trans
192.0.2.4(vpls-id 100) rmt LN

user@PE4> show vpls connections
Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down NP -- interface hardware not present
CM -- control-word mismatch -> -- only outbound connection is up
CN -- circuit not provisioned <- -- only inbound connection is up
OR -- out of range Up -- operational
OL -- no outgoing label Dn -- down
LD -- local site signaled down CF -- call admission control failure
RD -- remote site signaled down SC -- local and remote site ID collision
LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status IL -- no incoming label
MM -- MTU mismatch MI -- Mesh-Group ID not available
BK -- Backup connection ST -- Standby connection
PF -- Profile parse failure PB -- Profile busy
RS -- remote site standby SN -- Static Neighbor
LB -- Local site not best-site RB -- Remote site not best-site
VM -- VLAN ID mismatch

Legend for interface status
Up -- operational
Dn -- down

Instance: ldp-vpls
VPLS-id: 100
Neighbor Type St Time last up # Up trans
192.0.2.2(vpls-id 100) rmt Up Oct 16 17:12:23 2012 1
 Remote PE: 192.0.2.2, Negotiated control-word: No
 Incoming label: 800001, Outgoing label: 800000
 Negotiated PW status TLV: No
 Local interface: vt-2/0/10.17825793, Status: Up, Encapsulation: ETHERNET
 Description: Intf - vpls ldp-vpls neighbor 192.0.2.2 vpls-id 100
192.0.2.3(vpls-id 100) rmt Up Oct 16 17:12:20 2012 1
 Remote PE: 192.0.2.3, Negotiated control-word: No
 Incoming label: 800000, Outgoing label: 800000
 Negotiated PW status TLV: No
 Local interface: vt-2/0/10.17825792, Status: Up, Encapsulation: ETHERNET
 Description: Intf - vpls ldp-vpls neighbor 192.0.2.3 vpls-id 100

```

**Meaning** On Device PE1, the BGP-VPLS connection to Device PE2 is up. In a steady-state condition, Device PE2 is the primary router and has all pseudowires terminating on it. Traffic flows from CE1 to PE1 to PE2 to PE4 to CE4.

On Device PE2, the BGP-VPLS connection to Device PE1 is up. The connection to Device PE3 is in the RN state. The LDP-VPLS connection to Device PE4 is up.

On Device PE3, all VPLS connections are in the LN state. This is expected because Device PE3 is the backup.

On Device PE4, the LDP-only VPLS router, the primary pseudowire to Device PE2 and the backup pseudowire to Device PE3 are in the up state.

## Manually Triggering a Switch from the Active Pseudowire to the Backup Pseudowire

**Purpose** Verify that when Device PE2 becomes unavailable, the traffic flow shifts to Device PE3.

**Action** 1. On Device PE2, deactivate the interfaces.

```
user@PE2# deactivate interfaces
user@PE2# commit
```

2. Rerun the **show vpls connections** command on all of the PE devices.

```
user@PE1> show vpls connections
Layer-2 VPN connections:
```

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -> -- only outbound connection is up           |
| CN -- circuit not provisioned    | <- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unknown connection status  | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not available              |
| BK -- Backup connection          | ST -- Standby connection                       |
| PF -- Profile parse failure      | PB -- Profile busy                             |
| RS -- remote site standby        | SN -- Static Neighbor                          |
| LB -- Local site not best-site   | RB -- Remote site not best-site                |
| VM -- VLAN ID mismatch           |                                                |

Legend for interface status

Up -- operational  
Dn -- down

Instance: h-vpls-PE1

Local site: PE1-vpls (2)

| connection-site | Type | St        | Time last up         | # Up trans |
|-----------------|------|-----------|----------------------|------------|
| 1               | rmt  | <b>Up</b> | Oct 17 12:24:01 2012 | 2          |

Remote PE: 192.0.2.3, Negotiated control-word: No  
Incoming label: 800000, Outgoing label: 800257  
Local interface: vt-2/0/10.84934656, Status: Up, Encapsulation: VPLS  
Description: Intf - vpls h-vpls-PE1 local site 2 remote site 1

```
user@PE2> show vpls connections
```

Layer-2 VPN connections:

Legend for connection status (St)

|                                |                                                |
|--------------------------------|------------------------------------------------|
| EI -- encapsulation invalid    | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch   | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down  | NP -- interface hardware not present           |
| CM -- control-word mismatch    | -> -- only outbound connection is up           |
| CN -- circuit not provisioned  | <- -- only inbound connection is up            |
| OR -- out of range             | Up -- operational                              |
| OL -- no outgoing label        | Dn -- down                                     |
| LD -- local site signaled down | CF -- call admission control failure           |

```

RD -- remote site signaled down SC -- local and remote site ID collision
LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status IL -- no incoming label
MM -- MTU mismatch MI -- Mesh-Group ID not available
BK -- Backup connection ST -- Standby connection
PF -- Profile parse failure PB -- Profile busy
RS -- remote site standby SN -- Static Neighbor
LB -- Local site not best-site RB -- Remote site not best-site
VM -- VLAN ID mismatch

```

#### Legend for interface status

```

Up -- operational
Dn -- down

```

Instance: h-vpls-PE2

BGP-VPLS State

Local site: PE2-vpls (1)

LDP-VPLS State

VPLS-id: 100

Mesh-group connections: h-vpls-PE2

| Neighbor               | Type | St | Time last up | # Up trans |
|------------------------|------|----|--------------|------------|
| 192.0.2.4(vpls-id 100) | rmt  | OL |              |            |

user@PE3> show vpls connections

Layer-2 VPN connections:

#### Legend for connection status (St)

```

EI -- encapsulation invalid NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down NP -- interface hardware not present
CM -- control-word mismatch -> -- only outbound connection is up
CN -- circuit not provisioned <- -- only inbound connection is up
OR -- out of range Up -- operational
OL -- no outgoing label Dn -- down
LD -- local site signaled down CF -- call admission control failure
RD -- remote site signaled down SC -- local and remote site ID collision
LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status IL -- no incoming label
MM -- MTU mismatch MI -- Mesh-Group ID not available
BK -- Backup connection ST -- Standby connection
PF -- Profile parse failure PB -- Profile busy
RS -- remote site standby SN -- Static Neighbor
LB -- Local site not best-site RB -- Remote site not best-site
VM -- VLAN ID mismatch

```

#### Legend for interface status

```

Up -- operational
Dn -- down

```

Instance: h-vpls-PE3

BGP-VPLS State

Local site: PE3-vpls (1)

| connection-site | Type | St | Time last up         | # Up trans |
|-----------------|------|----|----------------------|------------|
| 2               | rmt  | Up | Oct 17 12:24:01 2012 | 1          |

Remote PE: 192.0.2.1, Negotiated control-word: No

Incoming label: 800257, Outgoing label: 800000

Local interface: vt-2/0/10.135266304, Status: Up, Encapsulation: VPLS

Description: Intf - vpls h-vpls-PE3 local site 1 remote site 2

LDP-VPLS State

VPLS-id: 100

```

Mesh-group connections: h-vpls-PE3
Neighbor Type St Time last up # Up trans
192.0.2.4(vpls-id 100) rmt Up Oct 17 12:24:02 2012 1

Remote PE: 192.0.2.4, Negotiated control-word: No
Incoming label: 800000, Outgoing label: 800000
Negotiated PW status TLV: No
Local interface: vt-2/0/10.135266305, Status: Up, Encapsulation: ETHERNET

Description: Intf - vpls h-vpls-PE3 neighbor 192.0.2.4 vpls-id 100

```

```

user@PE4> show vpls connections
Layer-2 VPN connections:

```

Legend for connection status (St)

```

EI -- encapsulation invalid NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down NP -- interface hardware not present
CM -- control-word mismatch -> -- only outbound connection is up
CN -- circuit not provisioned <- -- only inbound connection is up
OR -- out of range Up -- operational
OL -- no outgoing label Dn -- down
LD -- local site signaled down CF -- call admission control failure
RD -- remote site signaled down SC -- local and remote site ID collision
LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status IL -- no incoming label
MM -- MTU mismatch MI -- Mesh-Group ID not available
BK -- Backup connection ST -- Standby connection
PF -- Profile parse failure PB -- Profile busy
RS -- remote site standby SN -- Static Neighbor
LB -- Local site not best-site RB -- Remote site not best-site
VM -- VLAN ID mismatch

```

Legend for interface status

```

Up -- operational
Dn -- down

```

Instance: ldp-vpls

```

VPLS-id: 100
Neighbor Type St Time last up # Up trans
192.0.2.2(vpls-id 100) rmt OL
192.0.2.3(vpls-id 100) rmt Up Oct 16 17:12:20 2012 1

Remote PE: 192.0.2.3, Negotiated control-word: No
Incoming label: 800000, Outgoing label: 800000
Negotiated PW status TLV: No
Local interface: vt-2/0/10.17825792, Status: Up, Encapsulation: ETHERNET

Description: Intf - vpls ldp-vpls neighbor 192.0.2.3 vpls-id 100

```

**Meaning** On Device PE1, the BGP-VPLS connection to Device PE3 is up. Traffic flows from CE1 to PE1 to PE3 to PE4 to CE4.

On Device PE2, the BGP-VPLS connection to Device PE1 is in the OL state.

On Device PE3, all VPLS connections are up.

On Device PE4, the VPLS connection to Device PE2 is in the OL state. The VPLS connection to Device PE3 is up.

If you reactivate the interfaces on Device PE2, the connections revert to their previous state and traffic flow.

### Checking Connectivity

---

**Purpose** Verify that Device CE1 can ping Device CE4.

**Action** user@CE1> ping 10.255.14.219

```
PING 10.255.14.219 (10.255.14.219): 56 data bytes
64 bytes from 10.255.14.219: icmp_seq=0 ttl=64 time=1.149 ms
64 bytes from 10.255.14.219: icmp_seq=1 ttl=64 time=0.779 ms
^C
--- 10.255.14.219 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.779/0.964/1.149/0.185 ms
```

**Meaning** The output shows that VPLS is operational.

### Checking the BGP Layer 2 VPN Routing Tables

---

**Purpose** Verify that the VPLS routes are learned from BGP.

**Action** user@PE1> show route table bgp.l2vpn.0  
bgp.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)  
+ = Active Route, - = Last Active, \* = Both

```
1:3:1:1/96
 *[BGP/170] 20:00:11, localpref 100, from 192.0.2.3
 AS path: I, validation-state: unverified
 > to 10.10.1.2 via fe-2/0/10.0
```

user@PE3> show route table bgp.l2vpn.0  
bgp.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)  
+ = Active Route, - = Last Active, \* = Both

```
1:1:2:1/96
 *[BGP/170] 20:00:11, localpref 100, from 192.0.2.1
 AS path: I, validation-state: unverified
 > to 10.10.1.1 via fe-2/0/10.0
```

### Checking the Layer 2 Circuit Routing Tables

---

**Purpose** Verify that the VPLS routes are learned from LDP.



**Action** user@PE3> **show route table l2circuit.0**  
 l2circuit.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)  
 + = Active Route, - = Last Active, \* = Both

```

192.0.2.4:NoCtrlWord:5:100:Local/96
 *[VPLS/7] 01:30:11, metric2 1
 > to 10.10.6.2 via fe-2/0/9.0
192.0.2.4:NoCtrlWord:5:100:Remote/96
 *[LDP/9] 20:41:57
 Discard

```

user@PE4> **show route table bgp.l2vpn.0**  
 l2circuit.0: 3 destinations, 3 routes (2 active, 0 holddown, 1 hidden)  
 + = Active Route, - = Last Active, \* = Both

```

192.0.2.3:NoCtrlWord:5:100:Local/96
 *[VPLS/7] 20:42:51, metric2 1
 > to 10.10.6.1 via fe-2/0/9.0
192.0.2.3:NoCtrlWord:5:100:Remote/96
 *[LDP/9] 20:41:57
 Discard

```

**Related  
Documentation**

- [Application Note: Demystifying H-VPLS](#)
- [Example: Configuring H-VPLS Without VLANs on page 693](#)
- [Example: Configuring H-VPLS With VLANs on page 681](#)
- [Redundant Pseudowires for Layer 2 Circuits and VPLS on page 177](#)
- [Configuring Redundant Pseudowires for Layer 2 Circuits and VPLS on page 179](#)

## Example: Configuring BGP-Based H-VPLS Using Different Mesh Groups for Each Spoke Router

This example shows how to configure the hierarchical virtual private LAN service (H-VPLS) using different mesh groups to provide H-VPLS functionality and provides steps for verifying the configuration. This is one type of H-VPLS configuration possible in the Juniper Networks implementation. For information about the alternate type of configuration see “[Example: Configuring LDP-Based H-VPLS Using a Single Mesh Group to Terminate the Layer 2 Circuits](#)” on page 675.

Using mesh groups improves LDP-based VPLS control plane scalability and avoids the requirement for a full mesh of LDP sessions. This example uses BGP-based VPLS.

This example is organized into the following sections:

- [Requirements on page 654](#)
- [Overview and Topology on page 654](#)
- [Configuration on page 655](#)

## Requirements

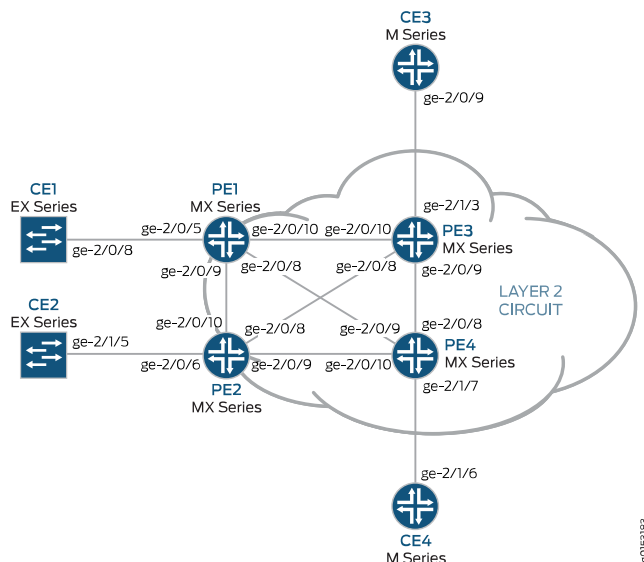
This example uses the following hardware components:

- Four MX Series 3D Universal Edge Routers for Router PE1, Router PE2, Router PE3, and Router PE4
- One M Series Multiservice Edge Router for Router CE4
- Two EX Series Ethernet Switches for Device CE1 and Device CE2
- One J Series Services Router for Router CE3

## Overview and Topology

Figure 55 on page 654 shows the physical topology used in this example.

Figure 55: Physical Topology of H-VPLS



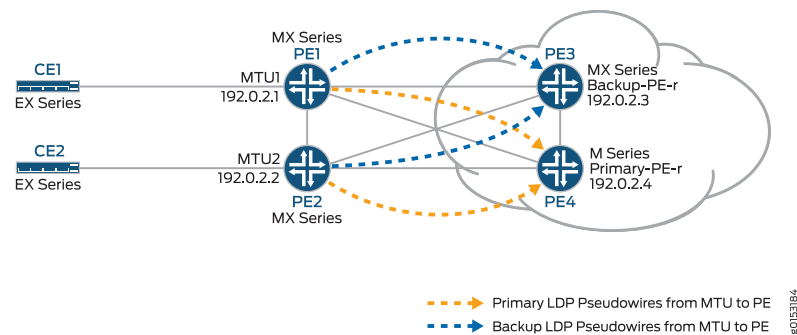
The following describes the base configuration used in this example:

- Router PE1 and Router PE2 are configured as MTU devices.
- Router PE3 and Router PE4 are configured as PE-r routers, each using an LDP-based VPLS routing instance.
- The LDP and OSPF protocols are configured on all of the MTU devices and PE-r routers.
- Core-facing interfaces are enabled with the MPLS address family.
- Optionally, the VPLS routing instances can be configured on PE-r routers with the **no-tunnel-interface** statement. This allows the routers to use a label-switched interface (LSI), which is useful if your routers do not have Tunnel Services PICs or built-in support for tunnel services.

- All of the routers are configured with loopback IP addresses.
- BGP is configured on the PE-r routers. Optionally, you can configure route reflection. This is useful for scaling internal BGP (IBGP). The BGP configuration includes the **signaling** statement at the `[edit protocols bgp group group-name family l2vpn]` hierarchy level to support Layer 2 VPN signaling using BGP.

Figure 56 on page 655 shows the logical topology used in this example.

Figure 56: Logical Topology of H-VPLS



In Figure 56 on page 655:

- The MTU devices (Router PE1 and Router PE2) have Layer 2 circuit connections to the PE-r routers (Router PE3 and Router PE4). For redundancy, a backup neighbor is configured for the Layer 2 circuit connections to the PE-r routers.
- The **l2circuit** statement in the `[edit protocols]` hierarchy is included on the MTU devices.
- A VPLS routing instance is configured on the PE-r routers.
- In the VPLS routing instance on the PE-r routers, mesh groups are created to terminate the Layer 2 circuit pseudowires that originate at the MTU devices.
- Each MTU device is configured with a different virtual circuit ID.
- Each PE-r router's mesh groups configuration includes VPLS ID values that match the virtual circuit IDs used on the MTU devices.

## Configuration

To configure H-VPLS with different mesh groups for each spoke PE-r router using BGP-based VPLS, perform the following tasks:

- [Configuring the Spoke MTU PE Routers on page 655](#)
- [Configuring the Hub PE \(PE-r\) on page 657](#)
- [Verifying the H-VPLS Operation on page 660](#)

### Configuring the Spoke MTU PE Routers

#### Step-by-Step Procedure

1. On Router PE1, configure the Gigabit Ethernet interface connected to Router CE1. Include the **encapsulation** statement and specify the **ethernet-ccc** option. Also

configure the logical interface by including the **family** statement and specifying the **ccc** option.

```
[edit interfaces]
ge-2/0/5 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
}
```

2. On Router PE1, configure the Layer 2 circuit by including the **neighbor** statement and specifying the IP address of Router PE3 as the neighbor. Configure the Gigabit Ethernet logical interface by including the **virtual-circuit-id** statement and specifying **100** as the ID. Also configure a backup neighbor for the Layer 2 circuit by including the **backup-neighbor** statement, specifying the loopback interface IP address of Router PE4 as the backup neighbor, and including the **standby** statement.

```
[edit protocols]
l2circuit {
 neighbor 192.0.2.3 {
 interface ge-2/0/5.0 {
 virtual-circuit-id 100;
 backup-neighbor 192.0.2.4 { # Backup H-VPLS PE router
 standby;
 }
 }
 }
}
```

3. On Router PE2, configure the Gigabit Ethernet interface connected to Router CE2. Include the **encapsulation** statement and specify the **ethernet-ccc** option. Also configure the logical interface by including the **family** statement and specifying the **ccc** option.

```
[edit interfaces]
ge-2/0/6 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
}
```

4. On Router PE2, configure the Layer 2 circuit by including the **neighbor** statement and specifying the IP address of Router PE3 as the neighbor. Configure the Gigabit Ethernet logical interface by including the **virtual-circuit-id** statement and specifying **200** as the ID. Configure the encapsulation by including the **encapsulation-type** statement and specifying the **ethernet** option. Also configure a backup neighbor for the Layer 2 circuit by including the **backup-neighbor** statement, specifying the loopback interface IP address of Router PE4 as the backup neighbor, and including the **standby** statement.

```
[edit protocols]
l2circuit {
 neighbor 192.0.2.3 {
 interface ge-1/0/2.0 {
 virtual-circuit-id 200; # different VC-ID
 }
 }
}
```

```

 encapsulation-type ethernet; # default encapsulation
 backup-neighbor 192.0.2.4 {
 standby;
 }
 }
}

```

### Configuring the Hub PE (PE-r)

#### Step-by-Step Procedure

1. On Router PE3 (the primary hub), configure the Gigabit Ethernet interface connected to Router CE3. Include the **encapsulation** statement and specify the **ethernet-vpls** option. Also configure the logical interface by including the **family vpls** statement.

```

[edit interfaces]
ge-2/0/0 {
 encapsulation ethernet-vpls;
 unit 0 {
 family vpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.3/24;
 }
 }
}

```

2. On Router PE4 (the backup hub), configure the Gigabit Ethernet interface connected to Router CE4. Include the **encapsulation** statement and specify the **ethernet-vpls** option. Also configure the logical interface by including the **family vpls** statement.

```

[edit interfaces]
ge-2/1/7 {
 encapsulation ethernet-vpls;
 unit 0 {
 description to_CE4;
 family vpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.4/24;
 }
 }
}

```

3. On PE-r Router PE3, configure the BGP-based VPLS routing instance by including the **instance-type** statement at the **[edit routing-instances H-VPLS]** hierarchy level and specifying the **vpls** option. Include the **interface** statement and specify the Gigabit Ethernet interface connected to Router CE3. Configure a route distinguisher to ensure that the route advertisement is unique by including the **route-distinguisher** statement and specifying **192.0.2.3:33** as the value. Also configure the VPN routing

and forwarding (VRF) route target to be included in the route advertisements to the other routers participating in the VPLS. To configure the VRF route target, include the **vrf-target** statement and specify **target:64510:2** as the value. Optionally, include the **no-tunnel-services** statement to enable the use of LSI interfaces, which is useful if the device does not have tunnel services. The **no-tunnel-services** statement is omitted in this example. Optionally, you can include the **site-range** statement to specify an upper limit on the maximum site identifier that can be accepted to allow a pseudowire to be brought up. The **site-range** statement is omitted in this example. We recommend using the default of 65,534.

Configure the VPLS protocol and the mesh groups for each MTU PE device.

To configure the VPLS protocol, include the **vpls** statement at the **[edit routing-instances H-VPLS protocols]** hierarchy level. Include the **site** statement and specify a name for the site. Include the **interface** statement and specify the Gigabit Ethernet interface connected to Device CE3.

Configuring mesh groups under the VPLS instance terminates the Layer 2 circuit into the VPLS instance. To configure each mesh group, include the **mesh-group** statement and specify the mesh group name. In this example, the mesh group name is the name of the MTU device associated with each mesh group. Include the **vpls-id** statement and specify the ID that matches the virtual circuit ID configured in [“Configuring the Spoke MTU PE Routers” on page 655](#). Also include the **neighbor** statement and specify the IP address of the spoke PE router associated with each mesh group. Optionally, include the **local-switching** statement if you are not using a full mesh of VPLS connections. The **local-switching** statement is useful if you are configuring a single mesh group and terminating multiple Layer 2 circuit pseudowires into it. The **local-switching** statement is omitted in this example.

```
routing-instances {
 H-VPLS {
 instance-type vpls;
 interface ge-2/1/3.0;
 route-distinguisher 192.0.2.3:33;
 vrf-target target:64510:2;
 protocols {
 vpls {
 site pe3 {
 site-identifier 3;
 interface ge-2/1/3.0;
 }
 mesh-group pe1 {
 vpls-id 100;
 neighbor 192.0.2.1;
 }
 mesh-group pe2 {
 vpls-id 200;
 neighbor 192.0.2.2;
 }
 }
 }
 }
}
```

4. On PE-r Router PE4, configure a routing instance like the one on Router PE3.

```
routing-instances {
 H-VPLS {
 instance-type vpls;
 interface ge-2/1/7.0;
 route-distinguisher 192.0.2.4:44;
 vrf-target target:64510:2;
 protocols {
 vpls {
 site pe4 {
 site-identifier 4;
 interface ge-2/1/7.0;
 }
 mesh-group pe1 {
 vpls-id 100;
 neighbor 192.0.2.1;
 }
 mesh-group pe2 {
 vpls-id 200;
 neighbor 192.0.2.2;
 }
 }
 }
 }
}
```

### Verifying the H-VPLS Operation

---

**Step-by-Step Procedure** This section describes the operational commands that you can use to validate that the H-VPLS is working as expected.



1. On Router PE1 and Router PE2, use the **show l2circuit connections** command to verify that the Layer 2 circuit to Router PE3 is **Up** and the Layer 2 circuit to Router PE4 is in **standby** mode.

The output also shows the assigned label, virtual circuit ID, and the **ETHERNET** encapsulation type.

```
user@PE1> show l2circuit connections
Layer-2 Circuit Connections:
```

Legend for connection status (St)

|                                 |                                      |
|---------------------------------|--------------------------------------|
| EI -- encapsulation invalid     | NP -- interface h/w not present      |
| MM -- mtu mismatch              | Dn -- down                           |
| EM -- encapsulation mismatch    | VC-Dn -- Virtual circuit Down        |
| CM -- control-word mismatch     | Up -- operational                    |
| VM -- vlan id mismatch          | CF -- Call admission control failure |
| OL -- no outgoing label         | IB -- TDM incompatible bitrate       |
| NC -- intf encaps not CCC/TCC   | TM -- TDM misconfiguration           |
| BK -- Backup Connection         | ST -- Standby Connection             |
| CB -- rcvd cell-bundle size bad | SP -- Static Pseudowire              |
| LD -- local site signaled down  | RS -- remote site standby            |
| RD -- remote site signaled down | XX -- unknown                        |

Legend for interface status

Up -- operational

Dn -- down

Neighbor: 192.0.2.3

| Interface          | Type | St        | Time last up         | # Up trans |
|--------------------|------|-----------|----------------------|------------|
| ge-2/0/5.0(vc 100) | rmt  | <b>Up</b> | Oct 18 15:55:07 2012 | 1          |

Remote PE: 192.0.2.3, Negotiated control-word: No  
Incoming label: 299840, Outgoing label: 800001  
Negotiated PW status TLV: No  
Local interface: ge-2/0/5.0, Status: Up, Encapsulation: **ETHERNET**

Neighbor: 192.0.2.4

| Interface          | Type | St        | Time last up | # Up trans |
|--------------------|------|-----------|--------------|------------|
| ge-2/0/5.0(vc 100) | rmt  | <b>ST</b> |              |            |

```
user@PE2> show l2circuit connections
```

Layer-2 Circuit Connections:

Legend for connection status (St)

|                                 |                                      |
|---------------------------------|--------------------------------------|
| EI -- encapsulation invalid     | NP -- interface h/w not present      |
| MM -- mtu mismatch              | Dn -- down                           |
| EM -- encapsulation mismatch    | VC-Dn -- Virtual circuit Down        |
| CM -- control-word mismatch     | Up -- operational                    |
| VM -- vlan id mismatch          | CF -- Call admission control failure |
| OL -- no outgoing label         | IB -- TDM incompatible bitrate       |
| NC -- intf encaps not CCC/TCC   | TM -- TDM misconfiguration           |
| BK -- Backup Connection         | ST -- Standby Connection             |
| CB -- rcvd cell-bundle size bad | SP -- Static Pseudowire              |
| LD -- local site signaled down  | RS -- remote site standby            |
| RD -- remote site signaled down | XX -- unknown                        |

Legend for interface status

Up -- operational

Dn -- down

Neighbor: 192.0.2.3

| Interface          | Type | St        | Time last up         | # Up trans |
|--------------------|------|-----------|----------------------|------------|
| ge-2/0/6.0(vc 200) | rmt  | <b>Up</b> | Oct 18 15:55:07 2012 | 1          |

Remote PE: 192.0.2.3, Negotiated control-word: No  
Incoming label: 299872, Outgoing label: 800002

```

Negotiated PW status TLV: No
Local interface: ge-2/0/6.0, Status: Up, Encapsulation: ETHERNET
Neighbor: 192.0.2.4
Interface Type St Time last up # Up trans
ge-2/0/6.0(vc 200) rmt ST

```

- On Router PE1 and Router PE2, use the **show ldp neighbor** command to verify that the targeted LDP sessions have been created between the loopback interface to the primary and backup H-VPLS hub neighbors.

```

user@PE1> show ldp neighbor
Address Interface Label space ID Hold time
10.10.3.2 ge-2/0/9.0 192.0.2.2:0 13
10.10.1.2 ge-2/0/10.0 192.0.2.3:0 10
192.0.2.3 lo0.0 192.0.2.3:0 36
192.0.2.4 lo0.0 192.0.2.4:0 39
10.10.9.2 ge-2/0/8.0 192.0.2.4:0 14

```

```

user@PE2> show ldp neighbor
Address Interface Label space ID Hold time
10.10.3.1 ge-2/0/10.0 192.0.2.1:0 12
10.10.5.2 ge-2/0/9.0 192.0.2.4:0 11
10.10.4.1 ge-2/0/8.0 192.0.2.3:0 11
192.0.2.3 lo0.0 192.0.2.3:0 39
192.0.2.4 lo0.0 192.0.2.4:0 38

```

- On Router PE3 and Router PE4, use the **show vpls connections** command to verify that the VPLS connection status is **Up** for both the LDP-based VPLS and the BGP-based VPLS Layer 2 circuits that are terminated.

```
user@PE3> show vpls connections
```

Layer-2 VPN connections:

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -> -- only outbound connection is up           |
| CN -- circuit not provisioned    | <- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unknown connection status  | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not available              |
| BK -- Backup connection          | ST -- Standby connection                       |
| PF -- Profile parse failure      | PB -- Profile busy                             |
| RS -- remote site standby        | SN -- Static Neighbor                          |
| LB -- Local site not best-site   | RB -- Remote site not best-site                |
| VM -- VLAN ID mismatch           |                                                |

Legend for interface status

Up -- operational  
Dn -- down

Instance: H-VPLS

**BGP-VPLS State**

Local site: pe3 (3)

```

connection-site Type St Time last up # Up trans
4 rmt Up Oct 18 15:58:39 2012 1
 Remote PE: 192.0.2.4, Negotiated control-word: No
 Incoming label: 800267, Outgoing label: 800266
 Local interface: vt-2/0/9.135266562, Status: Up, Encapsulation: VPLS
 Description: Intf - vpls H-VPLS local site 3 remote site 4

```

**LDP-VPLS State**

Mesh-group connections: pe1

```

Neighbor Type St Time last up # Up trans
192.0.2.1(vpls-id 100) rmt Up Oct 18 15:55:07 2012 1
 Remote PE: 192.0.2.1, Negotiated control-word: No
 Incoming label: 800001, Outgoing label: 299840
 Negotiated PW status TLV: No
 Local interface: vt-2/0/10.135266560, Status: Up, Encapsulation: ETHERNET
 Description: Intf - vpls H-VPLS neighbor 192.0.2.1 vpls-id 100

```

Mesh-group connections: pe2

```

Neighbor Type St Time last up # Up trans
192.0.2.2(vpls-id 200) rmt Up Oct 18 15:55:07 2012 1
 Remote PE: 192.0.2.2, Negotiated control-word: No
 Incoming label: 800002, Outgoing label: 299872
 Negotiated PW status TLV: No
 Local interface: vt-2/0/8.135266561, Status: Up, Encapsulation: ETHERNET
 Description: Intf - vpls H-VPLS neighbor 192.0.2.2 vpls-id 200

```

user@PE4> show vpls connections

Layer-2 VPN connections:

Legend for connection status (St)

```

EI -- encapsulation invalid NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down NP -- interface hardware not present
CM -- control-word mismatch -> -- only outbound connection is up
CN -- circuit not provisioned <- -- only inbound connection is up
OR -- out of range Up -- operational
OL -- no outgoing label Dn -- down
LD -- local site signaled down CF -- call admission control failure
RD -- remote site signaled down SC -- local and remote site ID collision
LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status IL -- no incoming label
MM -- MTU mismatch MI -- Mesh-Group ID not available
BK -- Backup connection ST -- Standby connection
PF -- Profile parse failure PB -- Profile busy
RS -- remote site standby SN -- Static Neighbor
LB -- Local site not best-site RB -- Remote site not best-site
VM -- VLAN ID mismatch

```

Legend for interface status

```

Up -- operational
Dn -- down

```

Instance: H-VPLS

BGP-VPLS State

Local site: pe4 (4)

```

connection-site Type St Time last up # Up trans
3 rmt Up Oct 18 15:58:39 2012 1
 Remote PE: 192.0.2.3, Negotiated control-word: No
 Incoming label: 800266, Outgoing label: 800267
 Local interface: vt-2/0/8.17826050, Status: Up, Encapsulation: VPLS
 Description: Intf - vpls H-VPLS local site 4 remote site 3

```

LDP-VPLS State

```

Mesh-group connections: pe1
Neighbor Type St Time last up # Up trans
192.0.2.1(vpls-id 100) rmt Up Oct 18 15:58:39 2012 1
Remote PE: 192.0.2.1, Negotiated control-word: No
Incoming label: 800002, Outgoing label: 299856
Negotiated PW status TLV: No
Local interface: vt-2/0/9.17826048, Status: Up, Encapsulation: ETHERNET
Description: Intf - vpls H-VPLS neighbor 192.0.2.1 vpls-id 100

```

```

Mesh-group connections: pe2
Neighbor Type St Time last up # Up trans
192.0.2.2(vpls-id 200) rmt Up Oct 18 15:58:39 2012 1
Remote PE: 192.0.2.2, Negotiated control-word: No
Incoming label: 800003, Outgoing label: 299888
Negotiated PW status TLV: No
Local interface: vt-2/0/10.17826049, Status: Up, Encapsulation: ETHERNET
Description: Intf - vpls H-VPLS neighbor 192.0.2.2 vpls-id 200

```

4. On Router PE3 and Router PE4, use the **show vpls flood** command to verify that the H-VPLS PE router created a flood group for each spoke PE site.

```

user@PE3> show vpls flood
Name: H-VPLS
CEs: 1
VEs: 3
Flood Routes:
 Prefix Type Owner NhType NhIndex
 0x300cc/51 FLOOD_GRP_COMP_NH __ves__ comp 1376
 0x300cf/51 FLOOD_GRP_COMP_NH __all_ces__ comp 744
 0x300d5/51 FLOOD_GRP_COMP_NH pe1 comp 1702
 0x300d3/51 FLOOD_GRP_COMP_NH pe2 comp 1544
 0x30001/51 FLOOD_GRP_COMP_NH __re_flood__ comp 740

```

```

user@PE4> show vpls flood
Name: H-VPLS
CEs: 1
VEs: 3
Flood Routes:
 Prefix Type Owner NhType NhIndex
 0x300d1/51 FLOOD_GRP_COMP_NH __ves__ comp 1534
 0x300d0/51 FLOOD_GRP_COMP_NH __all_ces__ comp 753
 0x300d6/51 FLOOD_GRP_COMP_NH pe1 comp 1378
 0x300d4/51 FLOOD_GRP_COMP_NH pe2 comp 1695
 0x30002/51 FLOOD_GRP_COMP_NH __re_flood__ comp 750

```

5. On Router PE3 and Router PE4, use the **show vpls mac-table** command to verify that MAC addresses of the CE devices have been learned.

```

user@PE3> show vpls mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

```

```

Routing instance : H-VPLS
Bridging domain : __H-VPLS__, VLAN : NA
 MAC MAC Logical NH RTR
 address flags interface Index ID
 00:21:59:0f:35:32 D vt-2/0/8.135266560
 00:21:59:0f:35:33 D ge-2/1/3.0
 00:21:59:0f:35:d4 D vt-2/0/9.135266561
 00:21:59:0f:35:d5 D vt-2/0/10.135266562

```

```

user@PE4> show vpls mac-table

```

MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC)

SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

```
Logical system : PE4
Routing instance : H-VPLS
Bridging domain : __H-VPLS__, VLAN : NA
MAC MAC Logical NH RTR
address flags interface Index ID
00:21:59:0f:35:32 D vt-2/0/8.17826050
00:21:59:0f:35:33 D vt-2/0/9.17826050
00:21:59:0f:35:d4 D vt-2/0/10.17826050
00:21:59:0f:35:d5 D ge-2/1/7.0
```

6. Make sure that the CE devices can ping each other.

```
user@CE1> ping 10.255.14.219 # ping sent from CE1 CE4
PING 10.255.14.219 (10.255.14.219): 56 data bytes
64 bytes from 10.255.14.219: icmp_seq=0 ttl=64 time=10.617 ms
64 bytes from 10.255.14.219: icmp_seq=1 ttl=64 time=9.224 ms
^C
--- 10.255.14.219 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 9.224/9.921/10.617/0.697 ms

user@CE2> ping 10.255.14.218 # ping sent from CE2 to CE3

PING 10.255.14.218 (10.255.14.218): 56 data bytes
64 bytes from 10.255.14.218: icmp_seq=0 ttl=64 time=1.151 ms
64 bytes from 10.255.14.218: icmp_seq=1 ttl=64 time=0.674 ms
^C
--- 10.255.14.218 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.674/0.913/1.151/0.238 ms
```

7. Check the relevant routing tables.

```
user@PE1> show route table l2circuit.0
l2circuit.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.3:NoCtrlWord:5:100:Local/96
 *[L2CKT/7] 00:12:16, metric2 1
 > to 10.10.1.2 via ge-2/0/10.0
192.0.2.3:NoCtrlWord:5:100:Remote/96
 *[LDP/9] 00:12:16
 Discard
192.0.2.4:NoCtrlWord:5:100:Local/96
 *[L2CKT/7] 00:12:10, metric2 1
 > to 10.10.9.2 via ge-2/0/8.0
192.0.2.4:NoCtrlWord:5:100:Remote/96
 *[LDP/9] 00:12:15
 Discard

user@PE2> show route table l2circuit.0
l2circuit.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.3:NoCtrlWord:5:200:Local/96
 *[L2CKT/7] 00:13:13, metric2 1
 > to 10.10.4.1 via ge-2/0/8.0
192.0.2.3:NoCtrlWord:5:200:Remote/96
```

```

*[LDP/9] 00:13:13
 Discard
192.0.2.4:NoCtrlWord:5:200:Local/96
*[L2CKT/7] 00:13:13, metric2 1
 > to 10.10.5.2 via ge-2/0/9.0
192.0.2.4:NoCtrlWord:5:200:Remote/96
*[LDP/9] 00:13:13
 Discard

user@PE3> show route table H-VPLS.l2vpn.0

H-VPLS.l2vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.3:33:3:1/96
*[L2VPN/170/-101] 03:19:26, metric2 1
 Indirect
192.0.2.4:44:4:1/96
*[BGP/170] 03:15:45, localpref 100, from 192.0.2.4
 AS path: I, validation-state: unverified
 > to 10.10.6.2 via ge-2/0/9.0

user@PE4> show route table H-VPLS.l2vpn.0

H-VPLS.l2vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.3:33:3:1/96
*[BGP/170] 03:21:17, localpref 100, from 192.0.2.3
 AS path: I, validation-state: unverified
 > to 10.10.6.1 via ge-2/0/9.0
192.0.2.4:44:4:1/96
*[L2VPN/170/-101] 03:17:47, metric2 1
 Indirect

```

**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 PE1 follows.

```

Router PE1 interfaces {
 ge-2/0/5 {
 encapsulation ethernet-ccc;
 unit 0 {
 description to_CE1;
 family ccc;
 }
 }
 ge-2/0/8 {
 unit 0 {
 description to_PE4;
 family inet {
 address 10.10.9.1/30;
 }
 family mpls;
 }
 }
 ge-2/0/9 {
 unit 0 {

```

```

 description to_PE2;
 family inet {
 address 10.10.3.1/30;
 }
 family mpls;
 }
}
ge-2/0/10 {
 unit 0 {
 description to_PE3;
 family inet {
 address 10.10.1.1/30;
 }
 family mpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.1/24;
 }
 }
}
}
protocols {
 mpls {
 interface ge-2/0/8.0;
 interface ge-2/0/9.0;
 interface ge-2/0/10.0;
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface lo0.0 {
 passive;
 }
 interface ge-2/0/8.0;
 interface ge-2/0/9.0;
 interface ge-2/0/10.0;
 }
 }
 ldp {
 interface ge-2/0/8.0;
 interface ge-2/0/9.0;
 interface ge-2/0/10.0;
 interface lo0.0;
 }
 l2circuit {
 neighbor 192.0.2.3 {
 interface ge-2/0/5.0 {
 virtual-circuit-id 100;
 backup-neighbor 192.0.2.4 {
 standby;
 }
 }
 }
 }
}

```

```
}
}
```

The relevant sample configuration for Router PE2 follows.

```
Router PE2 interfaces {
 ge-2/0/6 {
 encapsulation ethernet-ccc;
 unit 0 {
 description to_CE2;
 family ccc;
 }
 }
 ge-2/0/8 {
 unit 0 {
 description to_PE3;
 family inet {
 address 10.10.4.2/30;
 }
 family mpls;
 }
 }
 ge-2/0/9 {
 unit 0 {
 description to_PE4;
 family inet {
 address 10.10.5.1/30;
 }
 family mpls;
 }
 }
 ge-2/0/10 {
 unit 0 {
 description to_PE1;
 family inet {
 address 10.10.3.2/30;
 }
 family mpls;
 }
 }
 lo0 {
 unit 0 {
 family inet {
 address 192.0.2.2/24;
 }
 }
 }
}
protocols {
 mpls {
 interface ge-2/0/8.0;
 interface ge-2/0/9.0;
 interface ge-2/0/10.0;
 }
 ospf {
 traffic-engineering;
```



```

 area 0.0.0.0 {
 interface lo0.0 {
 passive;
 }
 interface ge-2/0/8.0;
 interface ge-2/0/9.0;
 interface ge-2/0/10.0;
 }
}
ldp {
 interface ge-2/0/8.0;
 interface ge-2/0/9.0;
 interface ge-2/0/10.0;
 interface lo0.0;
}
l2circuit {
 neighbor 192.0.2.3 {
 interface ge-2/0/6.0 {
 virtual-circuit-id 200;
 backup-neighbor 192.0.2.4 {
 standby;
 }
 }
 }
}
}
}

```

The relevant sample configuration for Router PE3 follows.

```

Router PE3 interfaces {
 ge-2/0/8 {
 unit 0 {
 description to_PE2;
 family inet {
 address 10.10.4.1/30;
 }
 family mpls;
 }
 }
 ge-2/0/9 {
 unit 0 {
 description to_PE4;
 family inet {
 address 10.10.6.1/30;
 }
 family mpls;
 }
 }
 ge-2/0/10 {
 unit 0 {
 description to_PE1;
 family inet {
 address 10.10.1.2/30;
 }
 family mpls;
 }
 }
}

```

```
}
ge-2/1/3 {
 encapsulation ethernet-vpls;
 unit 0 {
 description to_CE3;
 family vpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.3/24;
 }
 }
}
}
protocols {
 mpls {
 interface ge-2/0/8.0;
 interface ge-2/0/9.0;
 interface ge-2/0/10.0;
 }
 bgp {
 group internal-peers {
 type internal;
 local-address 192.0.2.3;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.4;
 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface lo0.0 {
 passive;
 }
 interface ge-2/0/8.0;
 interface ge-2/0/9.0;
 interface ge-2/0/10.0;
 }
 }
 ldp {
 interface ge-2/0/8.0;
 interface ge-2/0/9.0;
 interface ge-2/0/10.0;
 interface lo0.0;
 }
}
routing-instances {
 H-VPLS {
 instance-type vpls;
 interface ge-2/1/3.0;
 route-distinguisher 192.0.2.3:33;
 vrf-target target:64510:2;
 }
}
```

```

protocols {
 vpls {
 site pe3 {
 site-identifier 3;
 interface ge-2/1/3.0;
 }
 mesh-group pe1 {
 vpls-id 100;
 neighbor 192.0.2.1;
 }
 mesh-group pe2 {
 vpls-id 200;
 neighbor 192.0.2.2;
 }
 }
}
}
}
routing-options {
 autonomous-system 64510;
}

```

The relevant sample configuration for Router PE4 follows.

```

Router PE4 interfaces {
 ge-2/0/8 {
 unit 0 {
 description to_PE3;
 family inet {
 address 10.10.6.2/30;
 }
 family mpls;
 }
 }
 ge-2/0/9 {
 unit 0 {
 description to_PE1;
 family inet {
 address 10.10.9.2/30;
 }
 family mpls;
 }
 }
 ge-2/0/10 {
 unit 0 {
 description to_PE2;
 family inet {
 address 10.10.5.2/30;
 }
 family mpls;
 }
 }
 ge-2/1/7 {
 encapsulation ethernet-vpls;
 unit 0 {
 description to_CE4;
 }
 }
}

```

```
 family vpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.4/24;
 }
 }
}
protocols {
 mpls {
 interface ge-2/0/8.0;
 interface ge-2/0/9.0;
 interface ge-2/0/10.0;
 }
 bgp {
 group internal-peers {
 type internal;
 local-address 192.0.2.4;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.3;
 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface lo0.0 {
 passive;
 }
 interface ge-2/0/8.0;
 interface ge-2/0/9.0;
 interface ge-2/0/10.0;
 }
 }
 ldp {
 interface ge-2/0/8.0;
 interface ge-2/0/9.0;
 interface ge-2/0/10.0;
 interface lo0.0;
 }
}
routing-instances {
 H-VPLS {
 instance-type vpls;
 interface ge-2/1/7.0;
 route-distinguisher 192.0.2.4:44;
 vrf-target target:64510:2;
 protocols {
 vpls {
 site pe4 {
 site-identifier 4;
 interface ge-2/1/7.0;
 }
 }
 }
 }
}
```

```

 }
 mesh-group pe1 {
 vpls-id 100;
 neighbor 192.0.2.1;
 }
 mesh-group pe2 {
 vpls-id 200;
 neighbor 192.0.2.2;
 }
 }
 }
 }
 routing-options {
 autonomous-system 64510;
 }

```

The relevant sample configuration for Device CE1 follows.

```

Router CE1 interfaces {
 ge-2/0/8 {
 unit 0 {
 description to_PE1;
 family inet {
 address 172.16.0.1/24;
 }
 }
 }
 lo0 {
 unit 0 {
 family inet {
 address 10.255.14.214/32;
 }
 }
 }
}
protocols {
 ospf {
 area 0.0.0.0 {
 interface lo0.0 {
 passive;
 }
 interface ge-2/0/8.0;
 }
 }
}

```

The relevant sample configuration for Device CE2 follows.

```

Router CE2 interfaces {
 ge-2/1/5 {
 unit 0 {
 description to_PE2;
 family inet {
 address 172.16.0.2/24;
 }
 }
 }
}

```

```
 }
 lo0 {
 unit 0 {
 family inet {
 address 10.255.14.215/32;
 }
 }
 }
}
protocols {
 ospf {
 area 0.0.0.0 {
 interface lo0.0 {
 passive;
 }
 interface ge-2/1/5.0;
 }
 }
}
```

The relevant sample configuration for Device CE3 follows.

```
Router CE3 interfaces {
 ge-2/0/9 {
 unit 0 {
 description to_PE3;
 family inet {
 address 172.16.0.3/24;
 }
 }
 }
 lo0 {
 unit 0 {
 family inet {
 address 10.255.14.218/32;
 }
 }
 }
}
protocols {
 ospf {
 area 0.0.0.0 {
 interface lo0.0 {
 passive;
 }
 interface ge-2/0/9.0;
 }
 }
}
```

The relevant sample configuration for Device CE4 follows.

```
Router CE4 interfaces {
 ge-2/1/6 {
 unit 0 {
 description to_PE4;
 family inet {
```

```

 address 172.16.0.4/24;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 10.255.14.219/32;
 }
 }
}
protocols {
 ospf {
 area 0.0.0.0 {
 interface lo0.0 {
 passive;
 }
 interface ge-2/1/6.0;
 }
 }
}

```

**Related Documentation** • [Example: Configuring LDP-Based H-VPLS Using a Single Mesh Group to Terminate the Layer 2 Circuits on page 675](#)

## Example: Configuring LDP-Based H-VPLS Using a Single Mesh Group to Terminate the Layer 2 Circuits

This example shows how to configure a single mesh group to terminate the Layer 2 circuits into an LDP-based VPLS. This is one type of hierarchical virtual private LAN service (H-VPLS) configuration possible in the Juniper Networks implementation. For information about the alternate type of configuration see [“Example: Configuring BGP-Based H-VPLS Using Different Mesh Groups for Each Spoke Router” on page 653](#).

This example provides step-by-step configuration instructions and also provides steps for verifying and troubleshooting the configuration.

This example is organized into the following sections:

- [Requirements on page 675](#)
- [Overview and Topology on page 676](#)
- [Configuration on page 676](#)

### Requirements

This example uses the following hardware components:

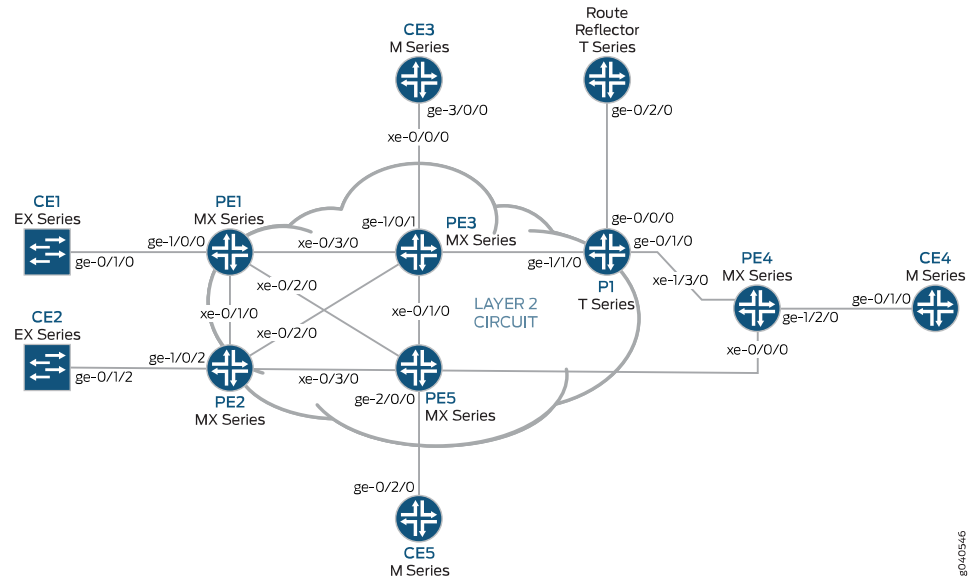
- Four MX Series 3D Universal Edge Routers for Routers PE1, PE2, PE3, and PE4
- Two M Series Multiservice Edge Routers for Routers CE4 and PE5

- Two EX Series Ethernet Switches for Devices CE1 and CE2
- Two T Series Core Routers for Routers P1 and the route reflector

## Overview and Topology

Figure 57 on page 676 shows the physical topology used in this example.

**Figure 57: Physical Topology of H-VPLS using a Single Mesh Group**



In Figure 57 on page 676:

- Local switching is used to switch traffic between Layer 2 circuit pseudowires from the different spoke PE routers.
- The spoke PE routers are configured with the same virtual circuit ID and VPLS ID pair in a mesh group.
- The spoke PE routers are configured in an LDP-signaled VPLS routing instance.
- The layer 2 circuits are terminated into the LDP-based VPLS.

## Configuration

To configure a single mesh group to terminate the Layer 2 circuits into an LDP-based VPLS, perform the following tasks:

- [Configuring the Spoke PE Routers on page 677](#)
- [Configuring the Hub PE Router on page 678](#)
- [Verification on page 679](#)



### Configuring the Spoke PE Routers

**Step-by-Step Procedure** Configure a single mesh group to terminate all the Layer 2 circuit pseudowires and enable local switching between the pseudowires.

1. On Router PE1, configure the Layer 2 circuit by including the **l2circuit** statement at the **[edit protocols]** hierarchy level. Include the **neighbor** statement and specify the IPv4 address of the hub PE router. Also configure the logical interface by including the **interface** statement and specify the interface connected to Router CE1.

Configure the virtual circuit ID by including the **virtual-circuit-id** statement and specifying **100** as the ID value at the **[edit protocols l2circuit neighbor 192.0.2.5 interface ge-1/0/0.0]** hierarchy level.

Configure the backup neighbor by including the **backup-neighbor** statement and specifying the IPv4 address of the backup hub PE router. Router PE3 is the backup neighbor in this example. Also include the **standby** statement at the **[edit protocols l2circuit neighbor 192.0.2.5 interface ge-1/0/0.0 backup-neighbor 192.0.2.3]** hierarchy level.

```
[edit protocols]
l2circuit {
 neighbor 192.0.2.5 {
 interface ge-1/0/0.0 {
 virtual-circuit-id 100;
 backup-neighbor 192.0.2.3 {
 standby;
 }
 }
 }
}
```

2. On Router PE2, configure the Layer 2 circuit by including the **l2circuit** statement at the **[edit protocols]** hierarchy level. Include the **neighbor** statement and specify the IPv4 address of the hub PE router. Configure the logical interface by including the **interface** statement and specifying the interface connected to Router CE2.

Configure the virtual circuit ID by including the **virtual-circuit-id** statement and specifying **100** as the ID value at the **[edit protocols l2circuit neighbor 192.0.2.5 interface ge-1/0/2.0]** hierarchy level. Include the **encapsulation** statement and specify **ethernet** as the type.

Configure the backup neighbor by including the **backup-neighbor** statement and specifying the IPv4 address of the backup hub PE router. Router PE3 is the backup neighbor in this example. Also include the **standby** statement at the **[edit protocols l2circuit neighbor 192.0.2.5 interface ge-1/0/0.0 backup-neighbor 192.0.2.3]** hierarchy level.

```
[edit protocols]
l2circuit {
 neighbor 192.0.2.5 {
 interface ge-1/0/2.0 {
 virtual-circuit-id 100;
 encapsulation-type ethernet;
 }
 }
}
```

```

 backup-neighbor 192.0.2.3 {
 standby;
 }
 }
}

```

3. On Router PE4, configure the Layer 2 circuit by including the **l2circuit** statement at the **[edit protocols]** hierarchy level. Include the **neighbor** statement and specify the IPv4 address of the hub PE router. Configure the logical interface by including the **interface** statement and specify the interface connected to Router CE4.

Configure the virtual circuit ID by including the **virtual-circuit-id** statement and specifying **100** as the ID value at the **[edit protocols l2circuit neighbor 192.0.2.5 interface ge-1/2/0.0]** hierarchy level.

Configure the backup neighbor by including the **backup-neighbor** statement and specifying the IPv4 address of the backup hub PE router. Router PE3 is the backup neighbor in this example. Also include the **standby** statement at the **[edit protocols l2circuit neighbor 192.0.2.5 interface ge-1/2/0.0 backup-neighbor 192.0.2.3]** hierarchy level.

```

[edit protocols]
l2circuit {
 neighbor 192.0.2.5 {
 interface ge-1/2/0.0 {
 virtual-circuit-id 100;
 backup-neighbor 192.0.2.3 {
 standby;
 }
 }
 }
}

```

### Configuring the Hub PE Router

**Step-by-Step Procedure** Configure a single mesh group to terminate all the Layer 2 circuit pseudowires and enable local switching between the pseudowires.

1. On Router PE3, configure the Gigabit Ethernet interface connected to Router CE3 by including the **encapsulation** statement and specifying the **ethernet-vpls** option. Also configure the logical interface by including the **family** statement and specifying the **vpls** option.

```

[edit interfaces]
ge-1/0/1 {
 encapsulation ethernet-vpls;
 unit 0 {
 family vpls;
 }
}

```

2. On Router PE3, configure the logical loopback interface by including the **family** statement and specifying the **inet** option. Include the **address** statement and specify the IPv4 address for the interface.

```
[edit interfaces]
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.3/24;
 }
 }
}
```

3. On Router PE3, configure the LDP-based VPLS routing instance by including the **instance-type** statement at the **[edit routing-instances H-VPLS]** hierarchy level and specifying the **vpls** option. Include the **interface** statement and specify the Gigabit Ethernet interface connected to Router CE3.

Configure the VPLS protocol by including the **vpls** statement at the **[edit routing-instances H-VPLS protocols]** hierarchy level. Include the **no-tunnel-services** statement to enable the router to use an LSI interface.

```
[edit routing-instances]
H-VPLS {
 instance-type vpls;
 interface ge-1/0/1.0;
 protocols {
 vpls {
 no-tunnel-services;
 }
 }
}
```

4. On Router PE3, configure the mesh group by including the **mesh-group** statement at the **[edit routing-instances H-VPLS protocols vpls]** hierarchy level and specifying **L2-Circuits** as the name of the group. Include the **vpls-id** statement and specify **100** as the ID value. Include the **local-switching** statement to enable the router to switch traffic between the pseudowires.

For each neighbor in the mesh group, include the **neighbor** statement and specify the IPv4 address of the spoke PE router.

```
[edit routing-instances H-VPLS protocols vpls]
mesh-group L2-Circuits {
 vpls-id 100; <<< Same VPLS ID on all MTUs
 local-switching; << Local-switching enabled
 neighbor 192.0.2.1; <<MTU IP addresses
 neighbor 192.0.2.2;
 neighbor 192.0.2.4;
}
```

## Verification

### Step-by-Step Procedure

1. On Router PE5, use the **show ldp neighbor** command to verify that LDP sessions have been created to each of the spoke PE routers.

```
user@PE5# show ldp neighbor
```

| Address   | Interface | Label space ID | Hold time |
|-----------|-----------|----------------|-----------|
| 192.0.2.1 | lo0.0     | 192.0.2.1:0    | 33        |

|           |       |             |    |
|-----------|-------|-------------|----|
| 192.0.2.2 | 100.0 | 192.0.2.2:0 | 37 |
| 192.0.2.4 | 100.0 | 192.0.2.4:0 | 39 |

- On Router PE5, use the **show vpls connections extensive** command to verify that the mesh group neighbor session is **Up**, that inbound and outbound labels have been assigned, that the VPLS ID is correct, and that the virtual tunnel interface is being used.

```
user@PE5# show vpls connections extensive
```

```
...
```

```
Instance: H-VPLS
```

```
Number of local interfaces: 1
```

```
Number of local interfaces up: 1
```

```
Number of VE mesh-groups: 2
```

```
Number of VE mesh-groups up: 1
```

```
ge-2/0/0.0
```

```
Mesh-group interfaces: L2-Circuits
```

```
State: Up ID: 2
```

```
vt-2/1/0.1048848 Intf - vpls H-VPLS neighbor 192.0.2.4 vpls-id 100
```

```
vt-2/1/0.1048849 Intf - vpls H-VPLS neighbor 192.0.2.2 vpls-id 100
```

```
vt-2/1/0.1048850 Intf - vpls H-VPLS neighbor 192.0.2.1 vpls-id 100
```

```
Mesh-group interfaces: __ves__
```

```
State: Dn ID: 0
```

```
Mesh-group connections: L2-Circuits
```

| Neighbor               | Type | St | Time last up        | # Up trans |
|------------------------|------|----|---------------------|------------|
| 192.0.2.4(vpls-id 100) | rmt  | Up | Jan 3 16:46:26 2010 | 1          |

```
Remote PE: 192.0.2.4, Negotiated control-word: No
```

```
Incoming label: 800011, Outgoing label: 301088
```

```
Local interface: vt-2/1/0.1048848, Status: Up, Encapsulation: ETHERNET
```

```
Description: Intf - vpls H-VPLS neighbor 192.0.2.4 vpls-id 100
```

```
Connection History:
```

```
Jan 3 16:46:26 2010 status update timer
```

```
Jan 3 16:46:26 2010 PE route changed
```

```
Jan 3 16:46:26 2010 In lbl Update 800011
```

```
Jan 3 16:46:26 2010 Out lbl Update 301088
```

```
Jan 3 16:46:26 2010 In lbl Update 800011
```

```
Jan 3 16:46:26 2010 loc intf up vt-2/1/0.1048848
```

|                        |     |    |                     |   |
|------------------------|-----|----|---------------------|---|
| 192.0.2.2(vpls-id 100) | rmt | Up | Jan 3 16:46:26 2010 | 1 |
|------------------------|-----|----|---------------------|---|

```
Remote PE: 192.0.2.2, Negotiated control-word: No
```

```
Incoming label: 800010, Outgoing label: 301488
```

```
Local interface: vt-2/1/0.1048849, Status: Up, Encapsulation: ETHERNET
```

```
Description: Intf - vpls H-VPLS neighbor 192.0.2.2 vpls-id 100
```

```
Connection History:
```

```
Jan 3 16:46:26 2010 status update timer
```

```
Jan 3 16:46:26 2010 PE route changed
```

```
Jan 3 16:46:26 2010 In lbl Update 800010
```

```
Jan 3 16:46:26 2010 Out lbl Update 301488
```

```
Jan 3 16:46:26 2010 In lbl Update 800010
```

```
Jan 3 16:46:26 2010 loc intf up vt-2/1/0.1048849
```

|                        |     |    |                     |   |
|------------------------|-----|----|---------------------|---|
| 192.0.2.1(vpls-id 100) | rmt | Up | Jan 3 16:46:26 2010 | 1 |
|------------------------|-----|----|---------------------|---|

```
Remote PE: 192.0.2.1, Negotiated control-word: No
```

```
Incoming label: 800009, Outgoing label: 301296
```

```
Local interface: vt-2/1/0.1048850, Status: Up, Encapsulation: ETHERNET
```

```
Description: Intf - vpls H-VPLS neighbor 192.0.2.1 vpls-id 100
```

```
Connection History:
```

```
Jan 3 16:46:26 2010 status update timer
```

```
Jan 3 16:46:26 2010 PE route changed
```

```
Jan 3 16:46:26 2010 In lbl Update 800009
```

```
Jan 3 16:46:26 2010 Out lbl Update 301296
```

```
Jan 3 16:46:26 2010 In lbl Update 800009
```

```
Jan 3 16:46:26 2010 loc intf up vt-2/1/0.1048850
```

- Related Documentation**
- [Example: Configuring BGP-Based H-VPLS Using Different Mesh Groups for Each Spoke Router on page 653](#)

## Example: Configuring H-VPLS With VLANs

This example shows how to configure the hierarchical virtual private LAN service (H-VPLS). VLANs are configured in this example.

- [Requirements on page 681](#)
- [Overview on page 681](#)
- [Configuration on page 683](#)
- [Verification on page 690](#)

### Requirements

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

### Overview

H-VPLS uses LDP-based VPLS to signal and establish pseudowires. LDP-based VPLS is defined in RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*. RFC 4762 also defines a hierarchical mode of operation for LDP VPLS called H-VPLS.

VPLS and H-VPLS are different with respect to scaling. VPLS requires a full mesh of tunnel label-switched paths (LSPs) among all of the provider edge (PE) routers that participate in the VPLS service. For each VPLS service,  $n*(n-1)/2$  pseudowires must be set up between the PE routers. In contrast, H-VPLS partitions the network into several edge domains that are interconnected using an MPLS core. Each edge device only needs to learn of one local PE device and therefore needs less routing table support. This has the potential to allow service providers to use relatively less costly devices (such as EX Series switches) at the customer edge.



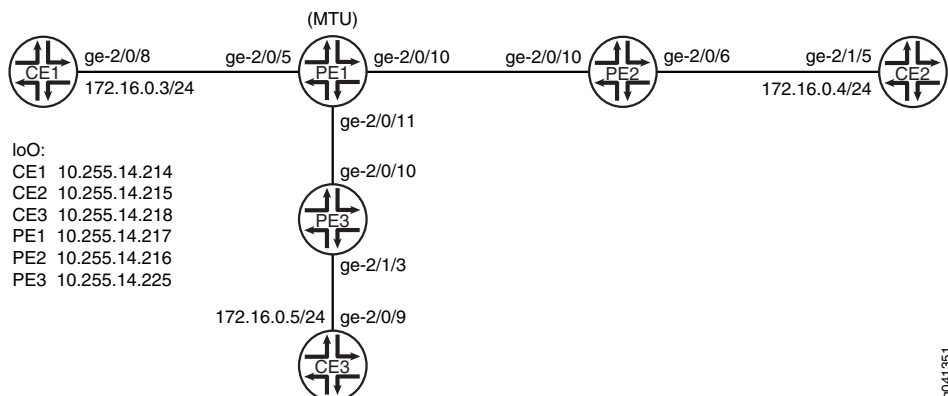
**NOTE:** As alternatives to H-VPLS, Juniper Networks offers other ways to address VPLS scalability. For more information, see [Application Note: Demystifying H-VPLS](#).

H-VPLS defines two roles or functionalities:

- PE-r—PE device that runs VPLS with other PE-r devices, but which also has pseudowires (it can be based on QinQ access) with another device called a multi-tenant unit (MTU), which provides the access layer.
- MTU—PE device that represents the access layer on the H-VPLS architecture and establishes pseudowires to one or more PE-r devices through which VPLS traffic is forwarded.

Figure 58 on page 682 shows the topology used in this example.

Figure 58: Basic H-VPLS With One MTU and Two PE-r Devices



The example shows one MTU (Device PE1) connected to two PE-r devices (Device PE2 and Device PE3).

The pseudowire between Device PE1 and Device PE3 is the primary or working path. The pseudowire between Device PE1 and Device PE2 is the backup path.

To support VLANs with H-VPLS, you must include the **output-vlan-map swap** statement in the configuration of the MTU device as a workaround to prevent a VLAN ID mismatch. Otherwise, the PE-r devices report a VLAN ID mismatch, as shown here:

```
user@PE2> show vpls connections
Layer-2 VPN connections:
```

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -> -- only outbound connection is up           |
| CN -- circuit not provisioned    | <- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unknown connection status  | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not available              |
| BK -- Backup connection          | ST -- Standby connection                       |
| PF -- Profile parse failure      | PB -- Profile busy                             |
| RS -- remote site standby        | SN -- Static Neighbor                          |
| LB -- Local site not best-site   | RB -- Remote site not best-site                |
| <b>VM -- VLAN ID mismatch</b>    |                                                |

Legend for interface status

Up -- operational  
Dn -- down

Instance: customer  
VPLS-id: 601

| Neighbor                   | Type | St | Time last up | # Up trans |
|----------------------------|------|----|--------------|------------|
| 10.255.14.217(vpls-id 601) | rmt  | VM |              |            |

“CLI Quick Configuration” on page 683 shows the configuration for all of the devices in Figure 58 on page 682. The section “Step-by-Step Procedure” on page 685 describes the steps on Device PE1 and Device PE2.

## 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 PE1**

```

set interfaces ge-2/0/5 vlan-tagging
set interfaces ge-2/0/5 encapsulation vlan-ccc
set interfaces ge-2/0/5 unit 601 encapsulation vlan-ccc
set interfaces ge-2/0/5 unit 601 vlan-id 601
set interfaces ge-2/0/5 unit 601 output-vlan-map swap
set interfaces ge-2/0/5 unit 601 family ccc
set interfaces ge-2/0/10 unit 0 family inet address 192.0.2.1/24
set interfaces ge-2/0/10 unit 0 family iso
set interfaces ge-2/0/10 unit 0 family mpls
set interfaces ge-2/0/11 unit 0 family inet address 192.0.2.2/24
set interfaces ge-2/0/11 unit 0 family iso
set interfaces ge-2/0/11 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.14.217/32
set interfaces lo0 unit 0 family iso address 49.0001.0102.5501.4217.00
set protocols mpls interface ge-2/0/10.0
set protocols mpls interface ge-2/0/11.0
set protocols isis level 1 disable
set protocols isis interface ge-2/0/10.0
set protocols isis interface ge-2/0/11.0
set protocols isis interface lo0.0
set protocols ldp interface ge-2/0/10.0
set protocols ldp interface ge-2/0/11.0
set protocols ldp interface lo0.0
set protocols l2circuit neighbor 10.255.14.225 interface ge-2/0/5.601 virtual-circuit-id 601
set protocols l2circuit neighbor 10.255.14.225 interface ge-2/0/5.601 encapsulation-type ethernet-vlan
set protocols l2circuit neighbor 10.255.14.225 interface ge-2/0/5.601 backup-neighbor 10.255.14.216 standby
set routing-options router-id 10.255.14.217

```

**Device PE2**

```

set interfaces ge-2/0/6 vlan-tagging
set interfaces ge-2/0/6 encapsulation vlan-vpls
set interfaces ge-2/0/6 unit 601 encapsulation vlan-vpls
set interfaces ge-2/0/6 unit 601 vlan-id 601
set interfaces ge-2/0/6 unit 601 family vpls
set interfaces ge-2/0/10 unit 0 family inet address 192.0.2.3/24
set interfaces ge-2/0/10 unit 0 family iso
set interfaces ge-2/0/10 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.14.216/32
set interfaces lo0 unit 0 family iso address 49.0001.0102.5501.4216.00
set protocols mpls interface ge-2/0/10.0

```

```
set protocols isis level 1 disable
set protocols isis interface ge-2/0/10.0
set protocols isis interface lo0.0
set protocols ldp interface ge-2/0/10.0
set protocols ldp interface lo0.0
set routing-instances customer instance-type vpls
set routing-instances customer interface ge-2/0/6.601
set routing-instances customer protocols vpls vpls-id 601
set routing-instances customer protocols vpls neighbor 10.255.14.217 encapsulation-type
 ethernet-vlan
set routing-options router-id 10.255.14.216
```

Device PE3

```
set interfaces ge-2/0/10 unit 0 family inet address 192.0.2.4/24
set interfaces ge-2/0/10 unit 0 family iso
set interfaces ge-2/0/10 unit 0 family mpls
set interfaces ge-2/1/3 vlan-tagging
set interfaces ge-2/1/3 encapsulation vlan-vpls
set interfaces ge-2/1/3 unit 601 encapsulation vlan-vpls
set interfaces ge-2/1/3 unit 601 vlan-id 601
set interfaces ge-2/1/3 unit 601 family vpls
set interfaces lo0 unit 0 family inet address 10.255.14.225/32
set interfaces lo0 unit 0 family iso address 49.0001.0102.5501.4225.00
set protocols mpls interface ge-2/0/10.0
set protocols isis level 1 disable
set protocols isis interface ge-2/0/10.0
set protocols isis interface lo0.0
set protocols ldp interface ge-2/0/10.0
set protocols ldp interface lo0.0
set routing-instances customer instance-type vpls
set routing-instances customer interface ge-2/1/3.601
set routing-instances customer protocols vpls vpls-id 601
set routing-instances customer protocols vpls neighbor 10.255.14.217 encapsulation-type
 ethernet-vlan
set routing-options router-id 10.255.14.225
```

Device CE1

```
set interfaces ge-2/0/8 vlan-tagging
set interfaces ge-2/0/8 unit 601 vlan-id 601
set interfaces ge-2/0/8 unit 601 family inet address 172.16.0.3/24
set interfaces lo0 unit 0 family inet address 10.255.14.214/32
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-2/0/8.601
```

Device CE2

```
set interfaces ge-2/1/5 vlan-tagging
set interfaces ge-2/1/5 unit 601 vlan-id 601
set interfaces ge-2/1/5 unit 601 family inet address 172.16.0.4/24
set interfaces lo0 unit 0 family inet address 10.255.14.215/32
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-2/1/5.601
```

Device CE3

```
set interfaces ge-2/0/9 vlan-tagging
set interfaces ge-2/0/9 unit 601 vlan-id 601
set interfaces ge-2/0/9 unit 601 family inet address 172.16.0.5/24
set interfaces lo0 unit 0 family inet address 10.255.14.218/32
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-2/0/9.601
```



**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 H-VPLS on the MTU device:

1. Configure the interfaces.

On the MTU device interface that connects to the customer edge, configure one of the circuit cross-connect (CCC) encapsulation types and the CCC address family. This enables Layer 2 circuits.

On the core-facing interfaces, enable MPLS labels. The ISO address is needed as well on the core-facing interfaces because IS-IS is used in the core.

```
[edit interfaces]
user@PE1# set ge-2/0/5 vlan-tagging
user@PE1# set ge-2/0/5 encapsulation vlan-ccc
user@PE1# set ge-2/0/5 unit 601 family ccc
user@PE1# set ge-2/0/5 unit 601 encapsulation vlan-ccc
user@PE1# set ge-2/0/5 unit 601 vlan-id 601
user@PE1# set ge-2/0/5 unit 601 output-vlan-map swap

user@PE1# set ge-2/0/10 unit 0 family inet address 192.0.2.1/24
user@PE1# set ge-2/0/10 unit 0 family iso
user@PE1# set ge-2/0/10 unit 0 family mpls

user@PE1# set ge-2/0/11 unit 0 family inet address 192.0.2.2/24
user@PE1# set ge-2/0/11 unit 0 family iso
user@PE1# set ge-2/0/11 unit 0 family mpls

user@PE1# set lo0 unit 0 family inet address 10.255.14.217/32
user@PE1# set lo0 unit 0 family iso address 49.0001.0102.5501.4217.00
```

2. Enable MPLS and LDP on the interfaces.

On the MTU device interfaces that connect to other PE devices, configure MPLS and LDP.

```
[edit protocols mpls]
user@PE1# set interface ge-2/0/10.0
user@PE1# set interface ge-2/0/11.0
```

```
[edit protocols ldp]
user@PE1# set interface ge-2/0/10.0
user@PE1# set interface ge-2/0/11.0
user@PE1# set interface lo0.0
```

3. Enable routing on the interfaces.

On the MTU device interfaces that connect to other PE devices, configure an interior gateway protocol (IGP), such as OSPF or IS-IS.

```
[edit protocols isis]
user@PE1# set level 1 disable
user@PE1# set interface ge-2/0/10.0
```

```
user@PE1# set interface ge-2/0/11.0
user@PE1# set interface lo0.0
```

4. Configure the Layer 2 circuit.

The neighbor 10.255.14.225 is Device PE3's loopback interface address. This sets up the working path.

The neighbor 10.255.14.216 is Device PE2's loopback interface address. This sets up the backup path.

The virtual circuit ID must match the VPLS ID that is configured on Device PE2 and Device PE3.

```
[edit protocols l2circuit neighbor 10.255.14.225 interface ge-2/0/5.601]
user@PE1# set virtual-circuit-id 601
user@PE1# set encapsulation-type ethernet-vlan
user@PE1# set backup-neighbor 10.255.14.216 standby
```

5. Configure the router ID.

```
[edit routing-options]
user@PE1# set router-id 10.255.14.217
```

#### 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 H-VPLS on the MTU device:

1. Configure the interfaces.

On the PE-r device interface that connects to the customer edge, configure one of the VPLS encapsulation types and the VPLS address family. This enables VPLS.

On the core-facing interfaces, enable MPLS labels. The ISO address is needed as well on the core-facing interfaces because IS-IS is used in the core.

```
[edit interfaces]
user@PE2# set ge-2/0/6 vlan-tagging
user@PE2# set ge-2/0/6 encapsulation vlan-vpls
user@PE2# set ge-2/0/6 unit 601 encapsulation vlan-vpls
user@PE2# set ge-2/0/6 unit 601 vlan-id 601
user@PE2# set ge-2/0/6 unit 601 family vpls

user@PE2# set ge-2/0/10 unit 0 family inet address 192.0.2.3/24
user@PE2# set ge-2/0/10 unit 0 family iso
user@PE2# set ge-2/0/10 unit 0 family mpls

user@PE2# set lo0 unit 0 family inet address 10.255.14.216/32
user@PE2# set lo0 unit 0 family iso address 49.0001.0102.5501.4216.00
```

2. Enable MPLS and LDP on the interfaces.

On the MTU device interfaces that connect to other PE devices, configure MPLS and LDP.

```
[edit protocols mpls]
```

```
user@PE2# set interface ge-2/0/10.0
```

```
[edit protocols ldp]
```

```
user@PE2# set interface ge-2/0/10.0
```

```
user@PE2# set interface lo0.0
```

3. Enable routing on the interfaces.

On the MTU device interfaces that connect to other PE devices, configure an interior gateway protocol (IGP), such as OSPF or IS-IS.

```
[edit protocols isis]
```

```
user@PE2# set level 1 disable
```

```
user@PE2# set interface ge-2/0/10.0
```

```
user@PE2# set interface lo0.0
```

4. Configure VPLS.

The **neighbor 10.255.14.217** statement points to Device PE1's loopback interface address.

The VPLS ID must match the virtual circuit ID that is configured on the MTU (Device PE1).

```
[edit routing-instances customer]
```

```
user@PE2# set instance-type vpls
```

```
user@PE2# set interface ge-2/0/6.601
```

```
user@PE2# set protocols vpls vpls-id 601
```

```
user@PE2# set protocols vpls neighbor 10.255.14.217 encapsulation-type
ethernet-vlan
```

5. Configure the router ID.

```
[edit routing-options]
```

```
user@PE2# set router-id 10.255.14.216
```

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

```
Device PE1 user@PE1# show interfaces
ge-2/0/5 {
 vlan-tagging;
 encapsulation vlan-ccc;
 unit 601 {
 encapsulation vlan-ccc;
 vlan-id 601;
 output-vlan-map swap;
 family ccc;
 }
}
ge-2/0/10 {
 unit 0 {
 family inet {
 address 192.0.2.1/24;
 }
 family iso;
```

```

 family mpls;
 }
}
ge-2/0/11 {
 unit 0 {
 family inet {
 address 192.0.2.2/24;
 }
 family iso;
 family mpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 10.255.14.217/32;
 }
 family iso {
 address 49.0001.0102.5501.4217.00;
 }
 }
}

```

user@PE1# show protocols

```

mpls {
 interface ge-2/0/10.0;
 interface ge-2/0/11.0;
}
isis {
 level 1 disable;
 interface ge-2/0/10.0;
 interface ge-2/0/11.0;
 interface lo0.0;
}
ldp {
 interface ge-2/0/10.0;
 interface ge-2/0/11.0;
 interface lo0.0;
}
l2circuit {
 neighbor 10.255.14.225 {
 interface ge-2/0/5.601 {
 virtual-circuit-id 601;
 encapsulation-type ethernet-vlan;
 backup-neighbor 10.255.14.216 {
 standby;
 }
 }
 }
}

```

user@PE1# show routing-options

```
router-id 10.255.14.217;
```

Device PE2

user@PE2# show interfaces

```
ge-2/0/6 {
```

```

vlan-tagging;
encapsulation vlan-vpls;
unit 601 {
 encapsulation vlan-vpls;
 vlan-id 601;
 family vpls;
}
}
ge-2/0/10 {
 unit 0 {
 family inet {
 address 192.0.2.3/24;
 }
 family iso;
 family mpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 10.255.14.216/32;
 }
 family iso {
 address 49.0001.0102.5501.4216.00;
 }
 }
}

user@PE2# show protocols
mpls {
 interface ge-2/0/10.0;
}
isis {
 level 1 disable;
 interface ge-2/0/10.0;
 interface lo0.0;
}
ldp {
 interface ge-2/0/10.0;
 interface lo0.0;
}

user@PE2# show routing-instances
customer {
 instance-type vpls;
 interface ge-2/0/6.601;
 protocols {
 vpls {
 vpls-id 601;
 neighbor 10.255.14.217 {
 encapsulation-type ethernet-vlan;
 }
 }
 }
}
}

```

```
user@PE2# show routing-options
router-id 10.255.14.216;
```

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

## Verification

Confirm that the configuration is working properly.

- [Verifying the Layer 2 Circuit on page 690](#)
- [Checking the VPLS Connections on page 691](#)
- [Checking Connectivity on page 692](#)
- [Manually Triggering a Switch from the Active Pseudowire to the Redundant Pseudowire on page 692](#)

### Verifying the Layer 2 Circuit

**Purpose** Verify that Layer 2 circuit is operational on the MTU device.

**Action** From operational mode, enter the **show l2circuit connections** command.

```
user@PE1> show l2circuit connections
Layer-2 Circuit Connections:
```

Legend for connection status (St)

|                                 |                                      |
|---------------------------------|--------------------------------------|
| EI -- encapsulation invalid     | NP -- interface h/w not present      |
| MM -- mtu mismatch              | Dn -- down                           |
| EM -- encapsulation mismatch    | VC-Dn -- Virtual circuit Down        |
| CM -- control-word mismatch     | Up -- operational                    |
| VM -- vlan id mismatch          | CF -- Call admission control failure |
| OL -- no outgoing label         | IB -- TDM incompatible bitrate       |
| NC -- intf encaps not CCC/TCC   | TM -- TDM misconfiguration           |
| BK -- Backup Connection         | ST -- Standby Connection             |
| CB -- rcvd cell-bundle size bad | SP -- Static Pseudowire              |
| LD -- local site signaled down  | RS -- remote site standby            |
| RD -- remote site signaled down | XX -- unknown                        |

Legend for interface status

Up -- operational  
Dn -- down

Neighbor: 10.255.14.216

| Interface            | Type | St | Time last up        | # Up trans |
|----------------------|------|----|---------------------|------------|
| ge-2/0/5.601(vc 601) | rmt  | Up | Oct 9 16:28:58 2012 | 1          |

Remote PE: 10.255.14.216, Negotiated control-word: No  
Incoming label: 299904, Outgoing label: 800001  
Negotiated PW status TLV: No  
Local interface: ge-2/0/5.601, Status: Up, Encapsulation: VLAN

Neighbor: 10.255.14.225

| Interface            | Type | St | Time last up | # Up trans |
|----------------------|------|----|--------------|------------|
| ge-2/0/5.601(vc 601) | rmt  | ST |              |            |

**Meaning** As expected, the Layer 2 circuit connection to Device PE3 is operational, and the connection to Device PE2 is in standby mode.

## Checking the VPLS Connections

**Purpose** Verify that the VPLS connections are operational on the PE-r devices.

**Action** From operational mode, enter the **show vpls connections** command.

```
user@PE2> show vpls connections
```

Layer-2 VPN connections:

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -> -- only outbound connection is up           |
| CN -- circuit not provisioned    | <- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unknown connection status  | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not available              |
| BK -- Backup connection          | ST -- Standby connection                       |
| PF -- Profile parse failure      | PB -- Profile busy                             |
| RS -- remote site standby        | SN -- Static Neighbor                          |
| LB -- Local site not best-site   | RB -- Remote site not best-site                |
| VM -- VLAN ID mismatch           |                                                |

Legend for interface status

Up -- operational  
Dn -- down

Instance: customer

VPLS-id: 601

| Neighbor                                                             | Type | St | Time last up        | # Up trans |
|----------------------------------------------------------------------|------|----|---------------------|------------|
| 10.255.14.217(vpls-id 601)                                           | rmt  | Up | Oct 9 16:29:02 2012 | 1          |
| Remote PE: 10.255.14.217, Negotiated control-word: No                |      |    |                     |            |
| Incoming label: 800001, Outgoing label: 299904                       |      |    |                     |            |
| Negotiated PW status TLV: No                                         |      |    |                     |            |
| Local interface: vt-2/0/10.84934914, Status: Up, Encapsulation: VLAN |      |    |                     |            |
| Description: Intf - vpls customer neighbor 10.255.14.217 vpls-id 601 |      |    |                     |            |

```
user@PE3> show vpls connections
```

Layer-2 VPN connections:

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -> -- only outbound connection is up           |
| CN -- circuit not provisioned    | <- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |

```
XX -- unknown connection status IL -- no incoming label
MM -- MTU mismatch MI -- Mesh-Group ID not available
BK -- Backup connection ST -- Standby connection
PF -- Profile parse failure PB -- Profile busy
RS -- remote site standby SN -- Static Neighbor
LB -- Local site not best-site RB -- Remote site not best-site
VM -- VLAN ID mismatch
```

#### Legend for interface status

```
Up -- operational
Dn -- down
```

Instance: customer

VPLS-id: 601

```
Neighbor Type St Time last up # Up trans
10.255.14.217(vpls-id 601) rmt Up Oct 9 16:29:02 2012 1
Remote PE: 10.255.14.217, Negotiated control-word: No
Incoming label: 800001, Outgoing label: 299920
Negotiated PW status TLV: No
Local interface: vt-2/0/10.68157698, Status: Up, Encapsulation: VLAN
Description: Intf - vpls customer neighbor 10.255.14.217 vpls-id 601
```

**Meaning** As expected, the VPLS connections are operational on both PE-r devices.

---

### Checking Connectivity

**Purpose** Verify that Device CE1 can ping Device CE3.

**Action**

```
user@CE1> ping 10.255.14.218
PING 10.255.14.218 (10.255.14.218): 56 data bytes
64 bytes from 10.255.14.218: icmp_seq=0 ttl=64 time=0.858 ms
64 bytes from 10.255.14.218: icmp_seq=1 ttl=64 time=0.527 ms
64 bytes from 10.255.14.218: icmp_seq=2 ttl=64 time=0.670 ms
^C
--- 10.255.14.218 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.527/0.685/0.858/0.136 ms
```

**Meaning** The output shows that H-VPLS is operational.

---

### Manually Triggering a Switch from the Active Pseudowire to the Redundant Pseudowire

**Purpose** Make sure that the pseudowire between Device PE1 and Device PE2 becomes operational.



**Action** user@CE1> [request l2circuit-switchover](#) virtual-circuit-id 601 neighbor 10.255.14.225  
 user@CE1> [ping 10.255.14.215](#)  
 PING 10.255.14.215 (10.255.14.215): 56 data bytes  
 64 bytes from 10.255.14.215: icmp\_seq=0 ttl=64 time=0.738 ms  
 64 bytes from 10.255.14.215: icmp\_seq=1 ttl=64 time=0.627 ms  
 64 bytes from 10.255.14.215: icmp\_seq=2 ttl=64 time=0.629 ms  
 ^C  
 --- 10.255.14.215 ping statistics ---  
 3 packets transmitted, 3 packets received, 0% packet loss  
 round-trip min/avg/max/stddev = 0.627/0.665/0.738/0.052 ms

**Meaning** The successful ping from Device CE1 to Device CE2 shows that the pseudowire between Device PE1 and PE2 is operational. Now, if you ping Device CE3 from Device CE1, the ping should fail.

- Related Documentation**
- [Application Note: Demystifying H-VPLS](#)
  - [Example: Configuring H-VPLS Without VLANs on page 693](#)
  - [Redundant Pseudowires for Layer 2 Circuits and VPLS on page 177](#)
  - [Configuring Redundant Pseudowires for Layer 2 Circuits and VPLS on page 179](#)

## Example: Configuring H-VPLS Without VLANs

This example shows how to configure the hierarchical virtual private LAN service (H-VPLS). No VLANs are configured in this example.

- [Requirements on page 693](#)
- [Overview on page 693](#)
- [Configuration on page 694](#)
- [Verification on page 701](#)

### Requirements

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

### Overview

H-VPLS uses LDP-based VPLS to signal and establish pseudowires. LDP-based VPLS is defined in RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*. RFC 4762 also defines a hierarchical mode of operation for LDP VPLS called H-VPLS.

VPLS and H-VPLS are different with respect to scaling. VPLS requires a full mesh of tunnel label-switched paths (LSPs) among all of the provider edge (PE) routers that participate in the VPLS service. For each VPLS service,  $n*(n-1)/2$  pseudowires must be set up between the PE routers. In contrast, H-VPLS partitions the network into several edge domains that are interconnected using an MPLS core. Each edge device only needs to learn of one local PE device and therefore needs less routing table support. This has

the potential to allow service providers to use relatively less costly devices (such as EX Series switches) at the customer edge.



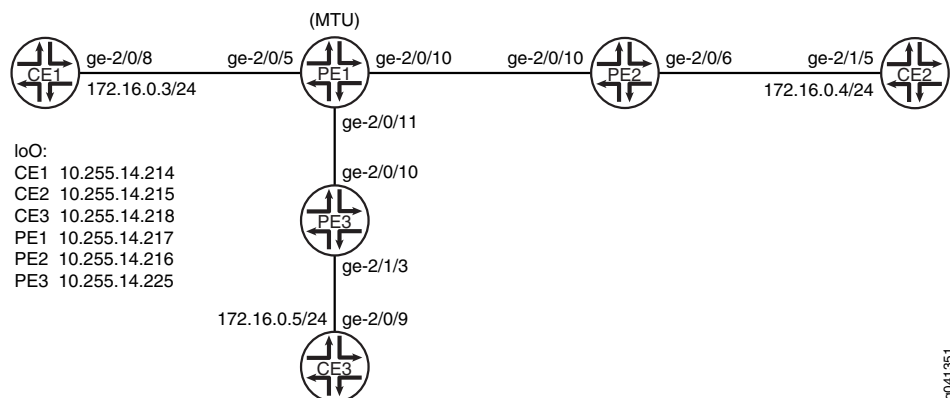
**NOTE:** As alternatives to H-VPLS, Juniper Networks offers other ways to address VPLS scalability. For more information, see [Application Note: Demystifying H-VPLS](#).

H-VPLS defines two roles or functionalities:

- PE-r—PE device that runs VPLS with other PE-r devices, but which also has pseudowires (it can be based on QinQ access) with another device called a multi-tenant unit (MTU), which provides the access layer.
- MTU—PE device that represents the access layer on the H-VPLS architecture and establishes pseudowires to one or more PE-r devices through which VPLS traffic is forwarded.

Figure 59 on page 694 shows the topology used in this example.

**Figure 59: Basic H-VPLS With One MTU and Two PE-r Devices**



The example shows one MTU (Device PE1) connected to two PE-r devices (Device PE2 and Device PE3).

The pseudowire between Device PE1 and Device PE3 is the primary or working path. The pseudowire between Device PE1 and Device PE2 is the backup path.

“CLI Quick Configuration” on page 694 shows the configuration for all of the devices in Figure 59 on page 694. The section “Step-by-Step Procedure” on page 696 describes the steps on Device PE1 and Device PE2.

## 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 PE1
set interfaces ge-2/0/5 encapsulation ethernet-ccc
set interfaces ge-2/0/5 unit 0 family ccc
set interfaces ge-2/0/10 unit 0 family inet address 192.0.2.1/24
set interfaces ge-2/0/10 unit 0 family iso
set interfaces ge-2/0/10 unit 0 family mpls
set interfaces ge-2/0/11 unit 0 family inet address 192.0.2.2/24
set interfaces ge-2/0/11 unit 0 family iso
set interfaces ge-2/0/11 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.14.217/32
set interfaces lo0 unit 0 family iso address 49.0001.0102.5501.4217.00
set protocols mpls interface ge-2/0/10.0
set protocols mpls interface ge-2/0/11.0
set protocols isis level 1 disable
set protocols isis interface ge-2/0/10.0
set protocols isis interface ge-2/0/11.0
set protocols isis interface lo0.0
set protocols ldp interface ge-2/0/10.0
set protocols ldp interface ge-2/0/11.0
set protocols ldp interface lo0.0
set protocols l2circuit neighbor 10.255.14.225 interface ge-2/0/5.0 virtual-circuit-id 601
set protocols l2circuit neighbor 10.255.14.225 interface ge-2/0/5.0 backup-neighbor
 10.255.14.216 standby
set routing-options router-id 10.255.14.217

Device PE2
set interfaces ge-2/0/6 encapsulation ethernet-vpls
set interfaces ge-2/0/6 unit 0 family vpls
set interfaces ge-2/0/10 unit 0 family inet address 192.0.2.3/24
set interfaces ge-2/0/10 unit 0 family iso
set interfaces ge-2/0/10 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.14.216/32
set interfaces lo0 unit 0 family iso address 49.0001.0102.5501.4216.00
set protocols mpls interface ge-2/0/10.0
set protocols isis level 1 disable
set protocols isis interface ge-2/0/10.0
set protocols isis interface lo0.0
set protocols ldp interface ge-2/0/10.0
set protocols ldp interface lo0.0
set routing-instances customer instance-type vpls
set routing-instances customer interface ge-2/0/6.0
set routing-instances customer protocols vpls vpls-id 601
set routing-instances customer protocols vpls neighbor 10.255.14.217
set routing-options router-id 10.255.14.216

Device PE3
set interfaces ge-2/1/3 encapsulation ethernet-vpls
set interfaces ge-2/1/3 unit 0 family vpls
set interfaces ge-2/0/10 unit 0 family inet address 192.0.2.4/24
set interfaces ge-2/0/10 unit 0 family iso
set interfaces ge-2/0/10 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.14.225/32
set interfaces lo0 unit 0 family iso address 49.0001.0102.5501.4225.00
set protocols mpls interface ge-2/0/10.0
set protocols isis level 1 disable
set protocols isis interface ge-2/0/10.0
set protocols isis interface lo0.0
set protocols ldp interface ge-2/0/10.0

```

```

set protocols ldp interface lo0.0
set routing-instances customer instance-type vpls
set routing-instances customer interface ge-2/1/3.0
set routing-instances customer protocols vpls vpls-id 601
set routing-instances customer protocols vpls neighbor 10.255.14.217
set routing-options router-id 10.255.14.225

```

**Device CE1**

```

set interfaces ge-2/0/8 unit 0 family inet address 172.16.0.3/24
set interfaces lo0 unit 0 family inet address 10.255.14.214/32
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-2/0/8.0

```

**Device CE2**

```

set interfaces ge-2/1/5 unit 0 family inet address 172.16.0.4/24
set interfaces lo0 unit 0 family inet address 10.255.14.215/32
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-2/1/5.0

```

**Device CE3**

```

set interfaces ge-2/0/9 unit 0 family inet address 172.16.0.5/24
set interfaces lo0 unit 0 family inet address 10.255.14.218/32
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-2/0/9.0

```

**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 H-VPLS on the MTU device:

1. Configure the interfaces.

On the MTU device interface that connects to the customer edge, configure one of the circuit cross-connect (CCC) encapsulation types and the CCC address family. This enables Layer 2 circuits.

On the core-facing interfaces, enable MPLS labels. The ISO address is needed as well on the core-facing interfaces because IS-IS is used in the core.

[edit interfaces]

```

user@PE1# set ge-2/0/5 encapsulation ethernet-ccc
user@PE1# set ge-2/0/5 unit 0 family ccc

```

```

user@PE1# set ge-2/0/10 unit 0 family inet address 192.0.2.1/24
user@PE1# set ge-2/0/10 unit 0 family iso
user@PE1# set ge-2/0/10 unit 0 family mpls

```

```

user@PE1# set ge-2/0/11 unit 0 family inet address 192.0.2.2/24
user@PE1# set ge-2/0/11 unit 0 family iso
user@PE1# set ge-2/0/11 unit 0 family mpls

```

```

user@PE1# set lo0 unit 0 family inet address 10.255.14.217/32
user@PE1# set lo0 unit 0 family iso address 49.0001.0102.5501.4217.00

```

2. Enable MPLS and LDP on the interfaces.

On the MTU device interfaces that connect to other PE devices, configure MPLS and LDP.

```
[edit protocols mpls]
user@PE1# set interface ge-2/0/10.0
user@PE1# set interface ge-2/0/11.0
```

```
[edit protocols ldp]
user@PE1# set interface ge-2/0/10.0
user@PE1# set interface ge-2/0/11.0
user@PE1# set interface lo0.0
```

3. Enable routing on the interfaces.

On the MTU device interfaces that connect to other PE devices, configure an interior gateway protocol (IGP), such as OSPF or IS-IS.

```
[edit protocols isis]
user@PE1# set level 1 disable
user@PE1# set interface ge-2/0/10.0
user@PE1# set interface ge-2/0/11.0
user@PE1# set interface lo0.0
```

4. Configure the Layer 2 circuit.

The neighbor 10.255.14.225 is Device PE3's loopback interface address. This sets up the working path.

The neighbor 10.255.14.216 is Device PE2's loopback interface address. This sets up the backup path.

The virtual circuit ID must match the VPLS ID that is configured on Device PE2 and Device PE3.

```
[edit protocols l2circuit neighbor 10.255.14.225 interface ge-2/0/5.0]
user@PE1# set virtual-circuit-id 601
user@PE1# set backup-neighbor 10.255.14.216 standby
```

5. Configure the router ID.

```
[edit routing-options]
user@PE1# set router-id 10.255.14.217
```

#### 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 H-VPLS on the MTU device:

1. Configure the interfaces.

On the PE-r device interface that connects to the customer edge, configure one of the VPLS encapsulation types and the VPLS address family. This enables VPLS.

On the core-facing interfaces, enable MPLS labels. The ISO address is needed as well on the core-facing interfaces because IS-IS is used in the core.

```
[edit interfaces]
user@PE2# set ge-2/0/6 encapsulation ethernet-vpls
```

```
user@PE2# set ge-2/0/6 unit 0 family vpls
```

```
user@PE2# set ge-2/0/10 unit 0 family inet address 192.0.2.3/24
```

```
user@PE2# set ge-2/0/10 unit 0 family iso
```

```
user@PE2# set ge-2/0/10 unit 0 family mpls
```

```
user@PE2# set lo0 unit 0 family inet address 10.255.14.216/32
```

```
user@PE2# set lo0 unit 0 family iso address 49.0001.0102.5501.4216.00
```

2. Enable MPLS and LDP on the interfaces.

On the MTU device interfaces that connect to other PE devices, configure MPLS and LDP.

```
[edit protocols mpls]
```

```
user@PE2# set interface ge-2/0/10.0
```

```
[edit protocols ldp]
```

```
user@PE2# set interface ge-2/0/10.0
```

```
user@PE2# set interface lo0.0
```

3. Enable routing on the interfaces.

On the MTU device interfaces that connect to other PE devices, configure an interior gateway protocol (IGP), such as OSPF or IS-IS.

```
[edit protocols isis]
```

```
user@PE2# set level 1 disable
```

```
user@PE2# set interface ge-2/0/10.0
```

```
user@PE2# set interface lo0.0
```

4. Configure VPLS.

The **neighbor 10.255.14.217** statement points to Device PE1's loopback interface address.

The VPLS ID must match the virtual circuit ID that is configured on the MTU (Device PE1).

```
[edit routing-instances customer]
```

```
user@PE2# set instance-type vpls
```

```
user@PE2# set interface ge-2/0/6.0
```

```
user@PE2# set protocols vpls vpls-id 601
```

```
user@PE2# set protocols vpls neighbor 10.255.14.217
```

5. Configure the router ID.

```
[edit routing-options]
```

```
user@PE2# set router-id 10.255.14.216
```

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

**Device PE1**

```
user@PE1# show interfaces
ge-2/0/5 {
 encapsulation ethernet-ccc;
```

```

 unit 0 {
 family ccc;
 }
}
ge-2/0/10 {
 unit 0 {
 family inet {
 address 192.0.2.1/24;
 }
 family iso;
 family mpls;
 }
}
ge-2/0/11 {
 unit 0 {
 family inet {
 address 192.0.2.2/24;
 }
 family iso;
 family mpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 10.255.14.217/32;
 }
 family iso {
 address 49.0001.0102.5501.4217.00;
 }
 }
}

```

```

user@PE1# show protocols
mpls {
 interface ge-2/0/10.0;
 interface ge-2/0/11.0;
}
isis {
 level 1 disable;
 interface ge-2/0/10.0;
 interface ge-2/0/11.0;
 interface lo0.0;
}
ldp {
 interface ge-2/0/10.0;
 interface ge-2/0/11.0;
 interface lo0.0;
}
l2circuit {
 neighbor 10.255.14.225 {
 interface ge-2/0/5.0 {
 virtual-circuit-id 601;
 }
 backup-neighbor 10.255.14.216 {
 standby;
 }
 }
}

```

```
 }
 }
}

user@PE1# show routing-options
router-id 10.255.14.217;

Device PE2 user@PE2# show interfaces
ge-2/0/6 {
 encapsulation ethernet-vpls;
 unit 0 {
 family vpls;
 }
}
ge-2/0/10 {
 unit 0 {
 family inet {
 address 192.0.2.3/24;
 }
 family iso;
 family mpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 10.255.14.216/32;
 }
 family iso {
 address 49.0001.0102.5501.4216.00;
 }
 }
}

user@PE2# show protocols
mpls {
 interface ge-2/0/10.0;
}
isis {
 level 1 disable;
 interface ge-2/0/10.0;
 interface lo0.0;
}
ldp {
 interface ge-2/0/10.0;
 interface lo0.0;
}

user@PE2# show routing-instances
customer {
 instance-type vpls;
 interface ge-2/0/6.0;
 protocols {
 vpls {
 vpls-id 601;
 neighbor 10.255.14.217;
 }
 }
}
```



```

 }
}

user@PE2# show routing-options
router-id 10.255.14.216;

```

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

## Verification

Confirm that the configuration is working properly.

- [Verifying the Layer 2 Circuit on page 701](#)
- [Checking the VPLS Connections on page 702](#)
- [Checking Connectivity on page 703](#)
- [Manually Triggering a Switch from the Active Pseudowire to the Redundant Pseudowire on page 703](#)

### Verifying the Layer 2 Circuit

**Purpose** Verify that the Layer 2 circuit is operational on the MTU device.

**Action** From operational mode, enter the **show l2circuit connections** command.

```

user@PE1> show l2circuit connections
Layer-2 Circuit Connections:

```

Legend for connection status (St)

|                                 |                                      |
|---------------------------------|--------------------------------------|
| EI -- encapsulation invalid     | NP -- interface h/w not present      |
| MM -- mtu mismatch              | Dn -- down                           |
| EM -- encapsulation mismatch    | VC-Dn -- Virtual circuit Down        |
| CM -- control-word mismatch     | Up -- operational                    |
| VM -- vlan id mismatch          | CF -- Call admission control failure |
| OL -- no outgoing label         | IB -- TDM incompatible bitrate       |
| NC -- intf encaps not CCC/TCC   | TM -- TDM misconfiguration           |
| BK -- Backup Connection         | ST -- Standby Connection             |
| CB -- rcvd cell-bundle size bad | SP -- Static Pseudowire              |
| LD -- local site signaled down  | RS -- remote site standby            |
| RD -- remote site signaled down | XX -- unknown                        |

Legend for interface status

Up -- operational  
Dn -- down

Neighbor: **10.255.14.216**

| Interface          | Type | St        | Time last up | # Up trans |
|--------------------|------|-----------|--------------|------------|
| ge-2/0/5.0(vc 601) | rmt  | <b>ST</b> |              |            |

Neighbor: **10.255.14.225**

| Interface          | Type | St        | Time last up        | # Up trans |
|--------------------|------|-----------|---------------------|------------|
| ge-2/0/5.0(vc 601) | rmt  | <b>Up</b> | Oct 5 19:38:15 2012 | 1          |

Remote PE: 10.255.14.225, Negotiated control-word: No

Incoming label: 299872, Outgoing label: 800001

Negotiated PW status TLV: No

Local interface: ge-2/0/5.0, Status: Up, Encapsulation: ETHERNET

**Meaning** As expected, the Layer 2 circuit connection to Device PE3 is operational, and the connection to Device PE2 is in standby mode.

## Checking the VPLS Connections

**Purpose** Verify that the VPLS connections are operational on the PE-r devices.

**Action** From operational mode, enter the **show vpls connections** command.

```
user@PE2> show vpls connections
```

Layer-2 VPN connections:

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -> -- only outbound connection is up           |
| CN -- circuit not provisioned    | <- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unknown connection status  | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not available              |
| BK -- Backup connection          | ST -- Standby connection                       |
| PF -- Profile parse failure      | PB -- Profile busy                             |
| RS -- remote site standby        | SN -- Static Neighbor                          |
| LB -- Local site not best-site   | RB -- Remote site not best-site                |
| VM -- VLAN ID mismatch           |                                                |

Legend for interface status

Up -- operational  
Dn -- down

Instance: customer

VPLS-id: 601

| Neighbor                                                                 | Type | St | Time last up        | # Up trans |
|--------------------------------------------------------------------------|------|----|---------------------|------------|
| 10.255.14.217(vpls-id 601)                                               | rmt  | Up | Oct 8 14:46:54 2012 | 1          |
| Remote PE: 10.255.14.217, Negotiated control-word: No                    |      |    |                     |            |
| Incoming label: 800001, Outgoing label: 299856                           |      |    |                     |            |
| Negotiated PW status TLV: No                                             |      |    |                     |            |
| Local interface: vt-2/0/10.84934913, Status: Up, Encapsulation: ETHERNET |      |    |                     |            |
| Description: Intf - vpls customer neighbor 10.255.14.217 vpls-id 601     |      |    |                     |            |

```
user@PE3> show vpls connections
```

Layer-2 VPN connections:

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -> -- only outbound connection is up           |
| CN -- circuit not provisioned    | <- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |

```

XX -- unknown connection status IL -- no incoming label
MM -- MTU mismatch MI -- Mesh-Group ID not available
BK -- Backup connection ST -- Standby connection
PF -- Profile parse failure PB -- Profile busy
RS -- remote site standby SN -- Static Neighbor
LB -- Local site not best-site RB -- Remote site not best-site
VM -- VLAN ID mismatch

```

Legend for interface status

Up -- operational

Dn -- down

Instance: customer

VPLS-id: 601

```

Neighbor Type St Time last up # Up trans
10.255.14.217(vpls-id 601) rmt Up Oct 8 14:46:54 2012 1
Remote PE: 10.255.14.217, Negotiated control-word: No
Incoming label: 800001, Outgoing label: 299872
Negotiated PW status TLV: No
Local interface: vt-2/0/10.68157697, Status: Up, Encapsulation: ETHERNET
Description: Intf - vpls customer neighbor 10.255.14.217 vpls-id 601

```

**Meaning** As expected, the VPLS connections are operational on both PE-r devices.

### Checking Connectivity

**Purpose** Verify that Device CE1 can ping Device CE3.

```

Action user@CE1> ping 10.255.14.218
PING 10.255.14.218 (10.255.14.218): 56 data bytes
64 bytes from 10.255.14.218: icmp_seq=0 ttl=64 time=0.858 ms
64 bytes from 10.255.14.218: icmp_seq=1 ttl=64 time=0.527 ms
64 bytes from 10.255.14.218: icmp_seq=2 ttl=64 time=0.670 ms
^C
--- 10.255.14.218 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.527/0.685/0.858/0.136 ms

```

**Meaning** The output shows that H-VPLS is operational.

### Manually Triggering a Switch from the Active Pseudowire to the Redundant Pseudowire

**Purpose** Make sure that the pseudowire between Device PE1 and Device PE2 becomes operational.

**Action**    user@CE1> [request l2circuit-switchover](#) virtual-circuit-id 601 neighbor 10.255.14.225  
user@CE1> [ping 10.255.14.215](#)  
PING 10.255.14.215 (10.255.14.215): 56 data bytes  
64 bytes from 10.255.14.215: icmp\_seq=0 ttl=64 time=0.738 ms  
64 bytes from 10.255.14.215: icmp\_seq=1 ttl=64 time=0.627 ms  
64 bytes from 10.255.14.215: icmp\_seq=2 ttl=64 time=0.629 ms  
^C  
--- 10.255.14.215 ping statistics ---  
3 packets transmitted, 3 packets received, 0% packet loss  
round-trip min/avg/max/stddev = 0.627/0.665/0.738/0.052 ms

**Meaning**    The successful ping from Device CE1 to Device CE2 shows that the pseudowire between Device PE1 and PE2 is operational. Now, if you ping Device CE3 from Device CE1, the ping should fail.

**Related Documentation**

- [Application Note: Demystifying H-VPLS](#)
- [Example: Configuring H-VPLS With VLANs on page 681](#)
- [Redundant Pseudowires for Layer 2 Circuits and VPLS on page 177](#)
- [Configuring Redundant Pseudowires for Layer 2 Circuits and VPLS on page 179](#)

# Configuring Multihoming

- [VPLS Multihoming Overview on page 705](#)
- [Advantages of Using Autodiscovery for VPLS Multihoming on page 708](#)
- [Example: Configuring FEC 129 BGP Autodiscovery for VPWS on page 708](#)
- [Example: Configuring BGP Autodiscovery for LDP VPLS on page 725](#)
- [Example: Configuring BGP Autodiscovery for LDP VPLS with User-Defined Mesh Groups on page 742](#)
- [VPLS Multihoming Reactions to Network Failures on page 752](#)
- [Configuring VPLS Multihoming \(FEC 128\) on page 753](#)
- [Example: VPLS Multihoming, Improved Convergence Time on page 756](#)
- [Example: Configuring VPLS Multihoming \(FEC 129\) on page 767](#)
- [Next-Generation VPLS for Multicast with Multihoming Overview on page 781](#)
- [Example: Next-Generation VPLS for Multicast with Multihoming on page 787](#)

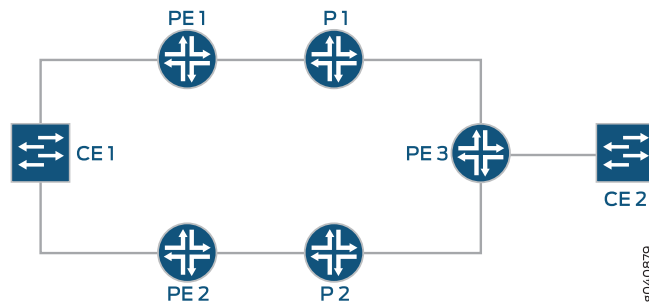
## VPLS Multihoming Overview

---

Virtual private LAN service (VPLS) multihoming enables you to connect a customer site to two or more PE routers to provide redundant connectivity. A redundant PE router can provide network service to the customer site as soon as a failure is detected. VPLS multihoming helps to maintain VPLS service and traffic forwarding to and from the multihomed site in the event of the following types of network failures:

- PE router to CE device link failure
- PE router failure
- MPLS-reachability failure between the local PE router and a remote PE router

Figure 60: CE Device Multihomed to Two PE Routers



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

Figure 20 on page 247 illustrates how a CE device could be multihomed to two PE routers. Device CE1 is multihomed to Routers PE1 and PE2. Device CE2 has two potential paths to reach Device CE1, but only one path is active at any one time. If Router PE1 were the designated VPLS edge (VE) device (also called a designated forwarder), BGP would signal a pseudowire from Router PE3 to Router PE1. If a failure occurred over this path, Router PE2 would be made the designated VE device, and BGP would re-signal the pseudowire from Router PE3 to Router PE2.

Multihomed PE routers advertise network layer reachability information (NLRI) for the multihomed site to the other PE routers in the VPLS network. The NLRI includes the site ID for the multihomed PE routers. For all of the PE routers multihomed to the same CE device, you need to configure the same site ID. The remote VPLS PE routers use the site ID to determine where to forward traffic addressed to the customer site. To avoid route collisions, the site ID shared by the multihomed PE routers must be different than the site IDs configured on the remote PE routers in the VPLS network.

Although you configure the same site ID for each of the PE routers multihomed to the same CE device, you can configure unique values for other parameters, such as the route distinguisher. These values help to determine which multihomed PE router is selected as the designated VE device to be used to reach the customer site.



**BEST PRACTICE:** We recommend that you configure unique route distinguishers for each multihomed PE router. Configuring unique route distinguishers helps with faster convergence when the connection to a primary multihomed PE router goes down. If you configure unique route distinguishers, the other PE routers in the VPLS network must maintain additional state for the multihomed PE routers.

Remote PE routers in the VPLS network need to determine which of the multihomed PE routers should forward traffic to reach the CE device. To make this determination, remote PE routers use the VPLS path-selection process to select one of the multihomed PE

routers based on its NLRI advertisement. Because remote PE routers pick only one of the NLRI advertisements, it establishes a pseudowire to only one of the multihomed PE routers, the PE router that originated the winning advertisement. This prevents multiple paths from being created between sites in the network, preventing the formation of Layer 2 loops. If the selected PE router fails, all PE routers in the network automatically switch to the backup PE router and establish new pseudowires to it.



**BEST PRACTICE:** To prevent the formation of Layer 2 loops between the CE devices and the multihomed PE routers, we recommend that you employ the Spanning Tree Protocol (STP) on your CE devices. Layer 2 loops can form due to incorrect configuration. Temporary Layer 2 loops can also form during convergence after a change in the network topology.

The PE routers run the BGP path selection procedure on locally originated and received Layer 2 route advertisements to establish that the routes are suitable for advertisement to other peers, such as BGP route reflectors. If a PE router in a VPLS network is also a route reflector, the path selection process for the multihomed site has no effect on the path selection process performed by this PE router for the purpose of reflecting Layer 2 routes. Layer 2 prefixes that have different route distinguishers are considered to have different NLRIs for route reflection. The VPLS path selection process enables the route reflector to reflect all routes that have different route distinguishers to the route reflector clients, even though only one of these routes is used to create the VPLS pseudowire to the multihomed site.

Junos OS supports VPLS multihoming for both FEC 128 and FEC 129. Support for FEC 129 is added in Junos OS Release 12.3.

#### Related Documentation

- [Configuring VPLS Multihoming \(FEC 128\) on page 753](#)
- [Example: Configuring VPLS Multihoming \(FEC 129\) on page 769](#)
- [Example: VPLS Multihoming, Improved Convergence Time on page 756](#)

## Advantages of Using Autodiscovery for VPLS Multihoming

---

Virtual private LAN service (VPLS) provides a multipoint-to-multipoint Ethernet service that can span one or more metropolitan areas and provides connectivity between multiple sites as if these sites were attached to the same Ethernet LAN.

VPLS uses an IP and MPLS service provider infrastructure. From a service provider's point of view, use of IP and MPLS routing protocols and procedures instead of the Spanning Tree Protocol (STP), and MPLS labels instead of VLAN IDs, significantly improves the scalability of the VPLS service.

It is frequently a requirement for a service provider to supply its customers with redundant connectivity to one or more sites. This capability is called multihoming.

VPLS multihoming enables you to connect a customer site to two or more PE routers to provide redundant connectivity. A redundant PE router can provide network service to the customer site as soon as a failure is detected. VPLS multihoming helps to maintain VPLS service and traffic forwarding to and from the multihomed site in the event of the following types of network failures:

- PE router to CE device link failure
- PE router failure
- MPLS-reachability failure between the local PE router and a remote PE router

The Junos<sup>®</sup> operating system (Junos OS) supports both forwarding equivalency class (FEC) 128 and FEC 129. FEC 128 requires manually configured pseudowires. FEC 129 uses VPLS autodiscovery to convey endpoint information. After PE routers are autodiscovered, pseudowires are created automatically.

VPLS multihoming with support for FEC 129 enables you to interoperate with other vendor's auto-discovery for LDP-signaled VPLS. This interoperability allows you to select the vendor that offers the best value.

### Related Documentation

- [VPLS Multihoming Overview on page 705](#)
- [Example: Configuring VPLS Multihoming \(FEC 129\) on page 769](#)

## Example: Configuring FEC 129 BGP Autodiscovery for VPWS

---

- [Understanding VPWS on page 708](#)
- [Understanding FEC 129 BGP Autodiscovery for VPWS on page 711](#)
- [Example: Configuring FEC 129 BGP Autodiscovery for VPWS on page 713](#)

### Understanding VPWS

Virtual private wire service (VPWS) Layer 2 VPNs employ Layer 2 services over MPLS to build a topology of point-to-point connections that connect end customer sites in a VPN. These Layer 2 VPNs provide an alternative to private networks that have been provisioned



by means of dedicated leased lines or by means of Layer 2 virtual circuits that employ ATM or Frame Relay. The service provisioned with these Layer 2 VPNs is known as VPWS. You configure a VPWS *instance* on each associated edge device for each VPWS Layer 2 VPN.

Traditional VPNs over Layer 2 circuits require the provisioning and maintenance of separate networks for IP and for VPN services. In contrast, VPWS enables the sharing of a provider's core network infrastructure between IP and Layer 2 VPN services, reducing the cost of providing those services.

Junos OS supports two types of VPWS Layer 2 VPNs:

- Kompella Layer 2 VPNs, which use BGP for autodiscovery and signaling.
- FEC 129 BGP autodiscovery for VPWS, which uses BGP for autodiscovery and LDP as the signaling protocol.

FEC 129 BGP autodiscovery for VPWS requires the **l2vpn-id**, **source-attachment-identifier**, and **target-attachment-identifier** statements. Kompella Layer 2 VPNs require the **site-identifier** and **remote-site-id** statements.

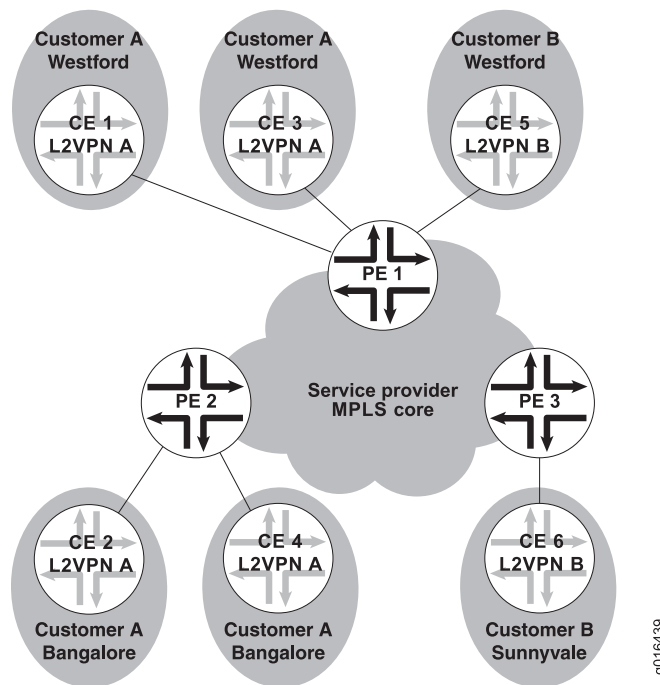


**NOTE:** VPWS creates pseudowires that emulate Layer 2 circuits. A virtual private LAN service (VPLS) network is similar to VPWS, but provides point-to-multipoint traffic forwarding in contrast to the VPWS Layer 2 VPN's point-to-point traffic forwarding. If you need point-to-multipoint service instead of point-to-point service, consider using VPLS instead of VPWS.

A VPWS Layer 2 VPN can have either a full-mesh or a hub-and-spoke topology. The tunneling mechanism in the core network typically is MPLS. However, VPWS can also use other tunneling protocols, such as GRE. VPWS is similar to Martini Layer 2 services over MPLS, and employs a similar encapsulation scheme for forwarding traffic.

Figure 39 on page 448 illustrates an example of a simple VPWS Layer 2 VPN topology.

Figure 61: VPWS Sample Topology



In this example, the service provider offers VPWS services to Customer A and Customer B. Customer A wants to create a full mesh of point-to-point links between Westford and Bangalore. Customer B needs only a single point-to-point link between Westford and Sunnyvale. The service provider uses BGP and MPLS signaling in the core, and creates a set of unidirectional pseudowires at each provider edge (PE) device to separately cross-connect each customer's Layer 2 circuits.

In order to provision this service, the provider configures two VPWS Layer 2 VPNs, Layer 2 VPN A and Layer 2 VPN B. The circuit cross-connect (CCC) encapsulation type (**ethernet-ccc** or **vlan-ccc**) is configured for each VPWS Layer 2 VPN. All interfaces in a given VPWS Layer 2 VPN must be configured with the VPWS Layer 2 VPN's encapsulation type.

Local and remote site information for the interfaces identifies the cross-connect. Local cross-connects are supported when the interfaces that are connected belong to two different sites configured in the same VPWS instance and on the same PE device.

BGP advertises reachability for the VPNs. The BGP configuration is similar to that used for other VPN services, such as Layer 3 VPNs and VPLS. MPLS is configured to set up base LSPs to the remote PE devices similarly to the other VPN services.

Junos OS provides VPWS support the following configuration methods:

- Pseudowires are manually configured using Forwarding Equivalence Class (FEC) 128.
- Pseudowires are signaled by LDP using FEC 129. This arrangement reduces the configuration burden that is associated with statically configured Layer 2 circuits while still using LDP as the underlying signaling protocol.

### Supported and Unsupported Features

---

Junos OS supports the following features with VPWS :

- Intra-AS VPWS functionality using BGP for autodiscovery and FEC 129 LDP for pseudowire signaling.
- Graceful Routing Engine switchover.
- Operation, administration, and maintenance (OAM) mechanisms, including Bidirectional Forwarding Detection and MPLS ping.
- FEC 128 LDP signaling with static configuration (in Junos OS this is configured within **protocols l2circuit**). With this option, there is no BGP autodiscovery.

Junos OS does not support the following VPWS functionality:

- Multihoming of customer sites to multiple PE devices using the BGP site model of multihoming.
- Terminating FEC 129 VPWS into a mesh group of an FEC 129 VPLS instance.
- Intra-AS VPWS functionality using BGP for autodiscovery and FEC 128 LDP for pseudowire signaling.
- FEC 129 VPWS without BGP autodiscovery.
- Static configuration of VPWS with FEC 129 signaling.
- Nonstop active routing.
- Multi-segment pseudowires.
- Interworking of FEC 128 and FEC 129 VPWS.
- Statically configured Layer 2 circuit-style pseudowire redundancy.
- Inter-AS deployments.

### Understanding FEC 129 BGP Autodiscovery for VPWS

The major functional components in a VPWS with FEC 129 are BGP, LDP, and the Layer 2 VPN module of Junos OS. BGP is responsible for distributing the local autodiscovery routes created on each PE device to all other PE devices. LDP is responsible for using the autodiscovery information provided by BGP to set up targeted LDP sessions over which to signal the pseudowires. The Layer 2 VPN is the glue that binds the BGP and LDP functionalities together.

### Supported Standards in FEC 129 BGP Autodiscovery for VPWS

---

The relevant RFCs for this feature are as follows:

- RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*
- RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*

### Routes and Routing Table Interaction in FEC 129 BGP Autodiscovery for VPWS

BGP, LDP, and Layer 2 VPNs interact through different types of routes installed in the *instance.l2vpn.0* table. The routes that are present in the table are autodiscovery routes and pseudowire routes.

- Autodiscovery routes are used by BGP to allow autodiscovery of remote source access individual identifiers (SAIs) (the sources of the point-to-point pseudowires) and PE device addresses. Autodiscovery routes are advertised when you configure the **l2vpn auto-discovery-only** address family.

The format of the autodiscovery routes is a combination of the route distinguisher and the SAI. For example: 10.255.0.1:100:0.0.0.1/96 AD.

[Table 13 on page 458](#) lists the route elements and the number of associated bytes allocated to each element.

**Table 19: Autodiscovery Route Format**

| Route Element | Bytes   |
|---------------|---------|
| RD            | 8 bytes |
| SAI           | 4 bytes |

The **l2vpn-id** of the FEC 129 VPWS instance is attached to the route in a BGP extended community. One autodiscovery route is advertised for each source attachment identifier (SAI) in the instance.

- Pseudowire routes are installed by the Layer 2 VPN (local) and LDP (remote) to represent the bidirectional components of the pseudowire. For example: NoCtrlWord:5:100:200:2:0.0.0.1/176. The format of the routes is described in [Table 14 on page 458](#).

**Table 20: Pseudowire Route Format**

| Field Name                                                                                  | Field Description |
|---------------------------------------------------------------------------------------------|-------------------|
| Pseudowire type + control word bit                                                          | 2 bytes           |
| Remote PE address                                                                           | 4 bytes           |
| Attachment group identifier (AGI)                                                           | 8 bytes           |
| The AGI field of the pseudowire route is always set to the <b>l2vpn-id</b> of the instance. |                   |
| SAI                                                                                         | 4 bytes           |
| Target attachment individual identifier (TAII)                                              | 4 bytes           |

### Layer 2 VPN Behavior in FEC 129 BGP Autodiscovery for VPWS

A Layer 2 VPN installs a locally generated autodiscovery route into the instance.l2vpn.0 table for every SAll configured in an FEC 129 VPWS instance. The extended community containing the **l2vpn-id** is attached when the route is added to the instance.l2vpn.0 table.

For each autodiscovered SAll from a remote neighbor where the **l2vpn-id** matches the local **l2vpn-id** and the received SAll matches a locally configured TAll, the Layer 2 VPN obtains an MPLS label and generates a pseudowire route and adds it to the instance.l2vpn.0 table. The remote PE address is copied from the BGP protocol next hop for the autodiscovery route.

The Layer 2 VPN module of Junos OS is responsible for installing the forwarding routes into the mpls.0 table as usual.

### BGP Autodiscovery Behavior in FEC 129 BGP Autodiscovery for VPWS

Local autodiscovery routes installed by the Layer 2 VPN in the instance.l2vpn.0 table are advertised by BGP to remote PE devices **sl2vpn auto-discovery-only** address family according to the instance and BGP export policies.

On the receiving side, BGP accepts autodiscovery routes from remote peers and installs them in the local bgp.l2vpn.0 table, if they are allowed by inbound policy. The route is installed, and a secondary route is imported into the instance.l2vpn.0 table when an import route target match between the route and instance is found.

### LDP Signaling Behavior in VPWS in FEC 129 BGP Autodiscovery for VPWS

LDP listens for routes from instance.l2vpn.0 for any instance configured for FEC 129 VPWS. These routes are identified by the **instance-type l2vpn** statement in the routing instance and the presence of the **l2vpn-id** statement.

When a BGP autodiscovery route is installed, LDP sets up a targeted session with the remote peer, where the peer address is identified as the protocol next hop of the BGP autodiscovery route.

When a pseudowire route is installed in the instance.l2vpn.0 table, LDP uses the parameters associated with the route to signal the creation of the pseudowire using FEC 129. Upon receiving an FEC 129 label mapping message from a remote peer, LDP installs the pseudowire route in the ldp.l2vpn.0 table.

Upon a successful **l2vpn-id** match with a configured FEC 129 VPWS instance, a secondary pseudowire route is imported to the instance.l2vpn.0 table. If an outgoing pseudowire has not already been set up when the incoming pseudowire signaling is received, LDP initiates the outgoing pseudowire creation as well.

### Example: Configuring FEC 129 BGP Autodiscovery for VPWS

This example shows how to configure the virtual private wire service (VPWS), where remote provider edge (PE) devices are automatically discovered dynamically by BGP, and pseudowires are signaled by LDP using FEC 129. This arrangement reduces the

configuration burden that is associated with statically configured Layer 2 circuits while still using LDP as the underlying signaling protocol.

- [Requirements on page 714](#)
- [Overview on page 714](#)
- [Configuration on page 718](#)
- [Verification on page 722](#)

## Requirements

This example requires Junos OS Release 13.2 or later on the PE devices.

## Overview

Because VPWS is a point-to-point service, FEC 129 VPWS routing instances are configured as **instance-type l2vpn**. As with FEC 129 VPLS, FEC 129 VPWS uses the **l2vpn-id** statement to define the Layer 2 VPN of which the routing instance is a member. The presence of the **l2vpn-id** statement designates that FEC 129 LDP signaling is used for the routing instance. The absence of **l2vpn-id** indicates that BGP signaling is used instead.

The point-to-point nature of VPWS requires that you specify the source access individual identifier (SAIL) and the target access individual identifier (TAIL). This SAIL-TAIL pair defines a unique pseudowire between two PE devices.

The SAIL is specified with the **source-attachment-identifier** statement within the FEC 129 VPWS routing instance. You configure the source attachment identifier and the interfaces to associate with that source attachment identifier. Under each interface, you can configure the TAIL with the **target-attachment-identifier** statement. If the configured target identifier matches a source identifier advertised by a remote PE device by way of a BGP autodiscovery message, the pseudowire between that source-target pair is signaled. If there is no match between an advertised source identifier and the configured target identifier, the pseudowire is not established.

### Sample: VPWS Configuration with Multiple Interfaces and Sites

```
routing-instances {
 FEC129-VPWS {
 instance-type l2vpn;
 interface ge-0/0/1.0;
 interface ge-0/0/2.0;
 interface ge-0/0/3.0;
 route-distinguisher 10.255.0.1:200;
 l2vpn-id l2vpn-id:100:200;
 vrf-target target:100:200;
 protocols l2vpn {
 site CUSTOMER-1 {
 source-attachment-identifier 1;
 interface ge-0/0/1.0 {
 target-attachment-identifier 2;
 }
 interface ge-0/0/2.0 {
 target-attachment-identifier 3;
 }
 }
 }
 }
}
```

```

 }
 }

```

You can configure multiple interfaces within a site, because each SAI-TAIL pair defines a unique pseudowire, as shown with pseudowires 1-2 and 1-3 in the sample configuration. Both the source and target access identifiers are 4-byte numbers and can only be configured in FEC 129 VPWS instances where the **instance-type** is **l2vpn** and the **l2vpn-id** configuration statement is present.

You can specify the source and target identifiers as plain unsigned integers in the range 1 through 4,292,967,295.

The Layer 2 circuit and Layer 2 VPN services allow many optional parameters to be included on a per-pseudowire basis. FEC 129 VPWS allows such parameters as MTU settings, community tagging, and inclusion of a control word, as shown in this sample configuration:

**Sample: VPWS  
Configuration with  
Optional Configuration  
Parameters**

```

routing-instances {
 FEC129-VPWS {
 instance-type l2vpn;
 interface ge-0/0/1.0;
 interface ge-0/0/2.0;
 interface ge-0/0/3.0;
 route-distinguisher 10.255.0.1:200;
 l2vpn-id l2vpn-id:100:200;
 vrf-target target:100:200;
 protocols l2vpn {
 site CUSTOMER-1 {
 source-attachment-identifier 1;
 community COMM;
 control-word;
 encapsulation-type ethernet;
 ignore-encapsulation-mismatch;
 ignore-mtu-mismatch;
 mtu 1500;
 no-control-word;
 interface ge-0/0/1.0 {
 target-attachment-identifier 2;
 }
 interface ge-0/0/2.0 {
 target-attachment-identifier 3;
 community COMM;
 control-word;
 encapsulation-type ethernet;
 ignore-encapsulation-mismatch;
 ignore-mtu-mismatch;
 mtu 1500;
 no-control-word;
 }
 }
 }
 }
}

```

When configured within the site, the defined parameters affect any pseudowire originating from that site. When configured under an interface, the defined parameters affect that single specific pseudowire. This allows you to manipulate the parameters across all pseudowires associated with a particular local site in one place in the configuration.

Like other point-to-point services, the interfaces configured as members of the FEC 129 VPWS instance must be configured for CCC encapsulation and the CCC address family, as shown here:

```
interfaces {
 ge-0/0/1 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
 }
 ge-0/0/2 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
 }
 ge-0/0/3 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
 }
}
```

You can use **vlan-ccc** instead of **ethernet-ccc**.

To support the basic FEC 129 VPWS functionality, the BGP sessions on the PE devices also need to be configured with the BGP **auto-discovery-only** address family to allow exchange of the autodiscovery routes. If traditional BGP VPLS or Layer 2 VPN service is also provisioned on the PE devices, the address family **l2vpn signaling** is also required, as shown here:

```
bgp {
 group pe {
 type internal;
 local-address 10.255.0.1;
 family l2vpn {
 auto-discovery-only;
 signaling;
 }
 neighbor 10.255.0.2;
 neighbor 10.255.0.3;
 }
}
```

The following configuration sample shows an FEC 129 VPWS routing instance with the operation, administration, and maintenance (OAM) (ping and BFD) configuration options:



**Sample: VPWS  
Configuration with  
OAM**

```

routing-instances {
 FEC129-VPWS {
 instance-type l2vpn;
 interface ge-0/0/1.0;
 route-distinguisher 10.255.0.1:200;
 l2vpn-id l2vpn-id:100:200;
 vrf-target target:100:200;
 protocols l2vpn {
 oam {
 ping-interval 600;
 bfd-liveness-detection {
 minimum-interval 200;
 }
 }
 }
 site CUSTOMER {
 source-attachment-identifier 1;
 oam {
 ping-interval 600;
 bfd-liveness-detection {
 minimum-interval 200;
 }
 }
 }
 interface ge-0/0/1.0 {
 oam {
 ping-interval 600;
 bfd-liveness-detection {
 minimum-interval 200;
 }
 }
 }
 target-attachment-identifier 2;
 }
}
}

```

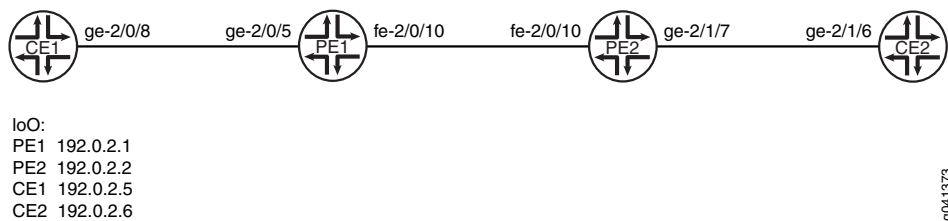
OAM options configured under **protocols l2vpn** apply to all sites and pseudowires in the routing instance. OAM options configured under a particular site apply to the pseudowires configured under that site. OAM options configured under a particular interface apply to the pseudowire configured under that interface.

***Topology Diagram***

Figure 42 on page 463 shows the topology used in this example.

This example uses a simple topology with two PE devices and two customer edge (CE) devices.

Figure 62: Simple VPWS Topology



g04-1373

“CLI Quick Configuration” on page 464 shows the configuration for all of the devices in Figure 42 on page 463. The section “Step-by-Step Procedure” on page 465 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-2/0/8 unit 0 description CE1_to_PE1
set interfaces ge-2/0/8 unit 0 family inet address 172.16.0.1/24
set interfaces lo0 unit 0 family inet address 192.0.2.5/24
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-2/0/8.0
```

**Device CE2**

```
set interfaces ge-2/1/6 unit 0 description CE2_to_PE2
set interfaces ge-2/1/6 unit 0 family inet address 172.16.0.4/24
set interfaces lo0 unit 0 family inet address 192.0.2.6/24
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-2/1/6.0
```

**Device PE1**

```
set interfaces ge-2/0/5 encapsulation ethernet-ccc
set interfaces ge-2/0/5 unit 0 description PE1_to_CE1
set interfaces ge-2/0/5 unit 0 family ccc
set interfaces fe-2/0/10 unit 0 description to_PE2
set interfaces fe-2/0/10 unit 0 family inet address 10.0.0.1/30
set interfaces fe-2/0/10 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 192.0.2.1/24
set protocols mpls interface fe-2/0/10.0
set protocols bgp local-address 192.0.2.1
set protocols bgp group pe-pe type internal
set protocols bgp group pe-pe family l2vpn auto-discovery-only
set protocols bgp group pe-pe family l2vpn signaling
set protocols bgp group pe-pe neighbor 192.0.2.2
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface fe-2/0/10.0
set protocols ldp interface fe-2/0/10.0
set protocols ldp interface lo0.0
set routing-instances FEC129-VPWS instance-type l2vpn
set routing-instances FEC129-VPWS interface ge-2/0/5.0
set routing-instances FEC129-VPWS route-distinguisher 192.0.2.1:100
set routing-instances FEC129-VPWS l2vpn-id l2vpn-id:100:100
```

```

set routing-instances FEC129-VPWS vrf-target target:100:100
set routing-instances FEC129-VPWS protocols l2vpn site ONE
 source-attachment-identifier 1
set routing-instances FEC129-VPWS protocols l2vpn site ONE interface ge-2/0/5.0
 target-attachment-identifier 2
set routing-options autonomous-system 64510

```

**Device PE2**

```

set interfaces ge-2/1/7 encapsulation ethernet-ccc
set interfaces ge-2/1/7 unit 0 description PE2_to_CE2
set interfaces ge-2/1/7 unit 0 family ccc
set interfaces fe-2/0/10 unit 0 description to_PE1
set interfaces fe-2/0/10 unit 0 family inet address 10.0.0.2/30
set interfaces fe-2/0/10 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 192.0.2.2/24
set protocols mpls interface fe-2/0/10.0
set protocols bgp local-address 192.0.2.2
set protocols bgp group pe-pe type internal
set protocols bgp group pe-pe family l2vpn auto-discovery-only
set protocols bgp group pe-pe family l2vpn signaling
set protocols bgp group pe-pe neighbor 192.0.2.1
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface fe-2/0/10.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ldp interface fe-2/0/10.0
set protocols ldp interface lo0.0
set routing-instances FEC129-VPWS instance-type l2vpn
set routing-instances FEC129-VPWS interface ge-2/1/7.0
set routing-instances FEC129-VPWS route-distinguisher 192.0.2.2:100
set routing-instances FEC129-VPWS l2vpn-id l2vpn-id:100:100
set routing-instances FEC129-VPWS vrf-target target:100:100
set routing-instances FEC129-VPWS protocols l2vpn site TWO
 source-attachment-identifier 2
set routing-instances FEC129-VPWS protocols l2vpn site TWO interface ge-2/1/7.0
 target-attachment-identifier 1
set routing-options autonomous-system 64510

```

**Step-by-Step  
Procedure**

To configure a FEC 129 VPWS:

1. Configure the interfaces.

```

[edit interfaces]
user@PE1# set ge-2/0/5 encapsulation ethernet-ccc
user@PE1# set ge-2/0/5 unit 0 description PE1_to_CE1
user@PE1# set ge-2/0/5 unit 0 family ccc

user@PE1# set fe-2/0/10 unit 0 description to_PE2
user@PE1# set fe-2/0/10 unit 0 family inet address 10.0.0.1/30
user@PE1# set fe-2/0/10 unit 0 family mpls

user@PE1# set lo0 unit 0 family inet address 192.0.2.1/24

```

2. Configure MPLS on the core-facing interface.

```

[edit protocols mpls]
user@PE1# set interface fe-2/0/10.0

```

## 3. Configure BGP.

```
[edit protocols bgp]
user@PE1# set local-address 192.0.2.1
user@PE1# set group pe-pe type internal
user@PE1# set group pe-pe family l2vpn auto-discovery-only
user@PE1# set group pe-pe family l2vpn signaling
user@PE1# set group pe-pe neighbor 192.0.2.2
```

## 4. Configure an interior gateway protocol, such as IS-IS or OSPF.

If you use OSPF, enable traffic engineering. Traffic engineering is supported by IS-IS by default.

```
[edit protocols ospf]
user@PE1# set traffic-engineering
user@PE1# set area 0.0.0.0 interface lo0.0 passive
user@PE1# set area 0.0.0.0 interface fe-2/0/10.0
```

## 5. Configure LDP on the core-facing interface and on the loopback interface.

```
[edit protocols ldp]
user@PE1# set interface fe-2/0/10.0
user@PE1# set interface lo0.0
```

## 6. Configure the VPWS routing instance.

LDP listens for routes from instance.l2vpn.0 for any instance configured for FEC 129 VPWS. These routes are identified by the **instance-type l2vpn** statement in the routing instance and the presence of the **l2vpn-id** statement.

Make sure that the **target-attachment-identifier** matches the **source-attachment-identifier** in the remote PE device's corresponding site. In this example, the pseudowire is established between Device PE1 and Device PE2. Device PE1 uses SAI 1 and TAI 2, while Device PE2 uses the opposite, SAI 2 and TAI 1.

```
[edit routing-instances FEC129-VPWS]
user@PE1# set instance-type l2vpn
user@PE1# set interface ge-2/0/5.0
user@PE1# set route-distinguisher 192.0.2.1:100
user@PE1# set l2vpn-id l2vpn-id:100:100
user@PE1# set vrf-target target:100:100
user@PE1# set protocols l2vpn site ONE source-attachment-identifier 1
user@PE1# set protocols l2vpn site ONE interface ge-2/0/5.0
target-attachment-identifier 2
```

## 7. Configure the autonomous system (AS) number.

```
[edit routing-options]
user@PE1# set autonomous-system 64510
```

## 8. If you are done configuring the device, commit the configuration.

```
[edit]
user@PE1# commit
```

**Results** From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols**, **show routing-instances**, and **show routing-options** command. If the output

does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```

user@PE1# show interfaces
ge-2/0/5 {
 encapsulation ethernet-ccc;
 unit 0 {
 description PE1_to_CE1;
 family ccc;
 }
}
fe-2/0/10 {
 unit 1 {
 description to_PE2;
 family inet {
 address 10.0.0.1/30;
 }
 family mpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.1/24;
 }
 }
}

user@PE1# show protocols
mpls {
 interface fe-2/0/10.0;
}
bgp {
 local-address 192.0.2.1;
 group pe-pe {
 type internal;
 family l2vpn {
 auto-discovery-only;
 inactive: signaling;
 }
 neighbor 192.0.2.2;
 }
}
ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface lo0.0 {
 passive;
 }
 interface fe-2/0/10.0;
 }
}
ldp {
 interface fe-2/0/10.0;
 interface lo0.0;
}

```

```

user@PE1# show routing-instances
FEC129-VPWS {
 instance-type l2vpn;
 interface ge-2/0/5.0;
 route-distinguisher 192.0.2.1:100;
 l2vpn-id l2vpn-id:100:100;
 vrf-target target:100:100;
 protocols {
 l2vpn {
 site ONE {
 source-attachment-identifier 1;
 interface ge-2/0/5.0 {
 target-attachment-identifier 2;
 }
 }
 }
 }
}

user@PE1# show routing-options
autonomous-system 64510;

```

## Verification

Confirm that the configuration is working properly.

- [Verifying the Routes on page 722](#)
- [Checking Connectivity Between the CE Devices on page 723](#)
- [Checking the VPWS Connections on page 724](#)
- [Checking Connectivity Between the PE Devices on page 725](#)

### Verifying the Routes

**Purpose** Verify that the expected routes are learned.

**Action** From operational mode, enter the **show route** command.

```

user@PE1> show route
inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.1/24 *[Direct/0] 6d 21:16:32
> via lo0.0
192.0.2.2/24 *[OSPF/10] 6d 21:15:31, metric 1
> to 10.0.0.2 via fe-2/0/10.0
10.0.0.0/30 *[Direct/0] 6d 21:16:31
> via fe-2/0/10.0
10.0.0.1/32 *[Local/0] 6d 21:16:32
Local via fe-2/0/10.0
203.0.113.0/24 *[OSPF/10] 6d 21:16:34, metric 1
MultiRecv

inet.3: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.2/24 *[LDP/9] 5d 22:25:19, metric 1
> to 10.0.0.2 via fe-2/0/10.0

```

```

mpls.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0 *[MPLS/0] 6d 21:16:33, metric 1
 Receive
1 *[MPLS/0] 6d 21:16:33, metric 1
 Receive
2 *[MPLS/0] 6d 21:16:33, metric 1
 Receive
13 *[MPLS/0] 6d 21:16:33, metric 1
 Receive
299808 *[LDP/9] 5d 22:25:19, metric 1
 > to 10.0.0.2 via fe-2/0/10.0, Pop
299808(S=0) *[LDP/9] 5d 22:25:19, metric 1
 > to 10.0.0.2 via fe-2/0/10.0, Pop
299824 *[L2VPN/7] 5d 22:25:18
 > via ge-2/0/5.0, Pop
ge-2/0/5.0 *[L2VPN/7] 5d 22:13:02, metric2 1
 > to 10.0.0.2 via fe-2/0/10.0, Push 299872

bgp.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.2:100:0.0.0.2/96 AD
 *[BGP/170] 6d 20:51:23, localpref 100, from 192.0.2.2
 AS path: I, validation-state: unverified
 > to 10.0.0.2 via fe-2/0/10.0

ldp.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.2:NoCtrlWord:5:100:100:0.0.0.2:0.0.0.1/176
 *[LDP/9] 5d 22:13:02
 Discard

FEC129-VPWS.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.1:100:0.0.0.1/96 AD
 *[L2VPN/170] 6d 20:53:26, metric2 1
 Indirect
192.0.2.2:100:0.0.0.2/96 AD
 *[BGP/170] 6d 20:51:23, localpref 100, from 192.0.2.2
 AS path: I, validation-state: unverified
 > to 10.0.0.2 via fe-2/0/10.0
192.0.2.2:NoCtrlWord:5:100:100:0.0.0.1:0.0.0.2/176
 *[L2VPN/7] 6d 20:51:23, metric2 1
 > to 10.0.0.2 via fe-2/0/10.0
192.0.2.2:NoCtrlWord:5:100:100:0.0.0.2:0.0.0.1/176
 *[LDP/9] 5d 22:13:02
 Discard

```

**Meaning** The output shows all the learned routes, including the autodiscovery (AD) routes.

### *Checking Connectivity Between the CE Devices*

**Purpose** Verify that Device CE1 can ping Device CE2.

**Action** user@CE1> ping 192.0.2.6  
 PING 192.0.2.6 (192.0.2.6): 56 data bytes  
 64 bytes from 192.0.2.6: icmp\_seq=0 ttl=64 time=0.679 ms  
 64 bytes from 192.0.2.6: icmp\_seq=1 ttl=64 time=0.524 ms  
 ^C  
 --- 192.0.2.6 ping statistics ---  
 2 packets transmitted, 2 packets received, 0% packet loss  
 round-trip min/avg/max/stddev = 0.524/0.602/0.679/0.078 ms

**Meaning** The output shows that the VPWS is operational.

### Checking the VPWS Connections

**Purpose** Make sure that all of the FEC 129 VPWS connections come up correctly.

**Action** user@PE1> show l2vpn connections  
 Layer-2 VPN connections:

Legend for connection status (St)  
 EI -- encapsulation invalid      NC -- interface encapsulation not CCC/TCC/VPLS  
 EM -- encapsulation mismatch    WE -- interface and instance encaps not same  
 VC-Dn -- Virtual circuit down   NP -- interface hardware not present  
 CM -- control-word mismatch    -> -- only outbound connection is up  
 CN -- circuit not provisioned   <- -- only inbound connection is up  
 OR -- out of range              Up -- operational  
 OL -- no outgoing label        Dn -- down  
 LD -- local site signaled down   CF -- call admission control failure  
 RD -- remote site signaled down   SC -- local and remote site ID collision  
 LN -- local site not designated   LM -- local site ID not minimum designated  
 RN -- remote site not designated   RM -- remote site ID not minimum designated  
 XX -- unknown connection status   IL -- no incoming label  
 MM -- MTU mismatch            MI -- Mesh-Group ID not available  
 BK -- Backup connection       ST -- Standby connection  
 PF -- Profile parse failure    PB -- Profile busy  
 RS -- remote site standby      SN -- Static Neighbor  
 LB -- Local site not best-site   RB -- Remote site not best-site  
 VM -- VLAN ID mismatch

Legend for interface status  
 Up -- operational  
 Dn -- down

Instance: FEC129-VPWS  
 L2vpn-id: 100:100  
**Local source-attachment-id: 1 (ONE)**

| Target-attachment-id | Type | St | Time last up         | # Up trans |
|----------------------|------|----|----------------------|------------|
| 2                    | rmt  | Up | Nov 28 16:16:14 2012 | 1          |

Remote PE: 192.0.2.2, Negotiated control-word: No  
 Incoming label: 299792, Outgoing label: 299792  
 Local interface: ge-2/0/5.0, Status: Up, Encapsulation: ETHERNET

**Meaning** As expected, the connection is up. The output includes the source attachment ID and the target attachment ID.



**Checking Connectivity Between the PE Devices**

**Purpose** Verify that Device PE1 can ping Device PE2. The `ping mpls l2vpn fec129` command accepts SAs and TAs as integers or IP addresses and also allows you to use the CE-facing interface instead of the other parameters (`instance`, `local-id`, `remote-id`, `remote-pe-address`).

**Action**

```

user@PE1> ping mpls l2vpn fec129 instance FEC129-VPWS remote-id 2 remote-pe-address
192.0.2.2 local-id 1
!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss

user@PE1> ping mpls l2vpn fec129 interface ge-2/0/5.0
!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss

```

**Meaning** The output shows that the VPWS is operational.

- Related Documentation**
- [Example: Configuring BGP Autodiscovery for LDP VPLS on page 725](#)
  - [Example: Configuring BGP Autodiscovery for LDP VPLS with User-Defined Mesh Groups on page 742](#)
  - [Example: Configuring VPLS Multihoming \(FEC 129\) on page 767](#)
  - [Introduction to Configuring Layer 2 VPNs on page 125](#)
  - [Configuring the Local Site on PE Routers in Layer 2 VPNs on page 126](#)

## Example: Configuring BGP Autodiscovery for LDP VPLS

This example describes how to configure BGP autodiscovery for LDP VPLS, as specified in forwarding equivalency class (FEC) 129. FEC 129 uses BGP autodiscovery to convey endpoint information, so you do not need to manually configure pseudowires.

- [Requirements on page 725](#)
- [Overview on page 726](#)
- [Configuration on page 728](#)
- [Verification on page 741](#)

### Requirements

This example uses the following hardware and software components:

- Four MX Series 3D Universal Edge Routers
- Junos OS Release 10.4R2 or later

If you are using M Series or T Series routers, the PE routers must have either virtual loopback tunnel (`vt`) interfaces or label-switched interfaces (LSIs). On M Series and T

Series routers, VPLS uses tunnel-based PICs to create virtual ports on **vt** interfaces. If you do not have a tunnel-based PIC installed on your M Series or T Series router, you can still configure VPLS by using LSIs to support the virtual ports. Use of LSIs requires Ethernet-based PICs installed in an Enhanced Flexible PIC Concentrator (FPC).

You do not need to use routers for the CE devices. For example, the CE devices can be EX Series Ethernet Switches.

## Overview

All PE routers in a VPLS network operate like a large, distributed Ethernet switch to provide Layer 2 services to attached devices. This example shows a minimum configuration for PE routers and CE devices to create an autodiscovered VPLS network. The topology consists of five routers: two PE routers, two CE routers, and an optional route reflector (RR). The PE routers use BGP to autodiscover two different VPLS instances that are configured on both PE routers. Then the PE routers use LDP to automatically signal two pseudowires between the discovered end points. Finally, the PE routers bring up both VPLS instances for forwarding traffic. Each CE device is configured with two VLANs, with each VLAN belonging to different VPLS instances in the PE routers.

This example includes the following settings:

- **auto-discovery-only**—Allows the router to process only the autodiscovery network layer reachability information (NLRI) update messages for LDP-based Layer 2 VPN and VPLS update messages (BGP\_L2VPN\_AD\_NLRI) (FEC 129). Specifically, the **auto-discovery-only** statement notifies the routing process (rpd) to expect autodiscovery-related NLRI messages so that information can be deciphered and used by LDP and VPLS. You can configure this statement at the global, group, and neighbor levels for BGP. The **auto-discovery-only** statement must be configured on all PE routers in the VPLS. If you configure route reflection, the **auto-discovery-only** statement is also required on P routers that act as the route reflector in supporting FEC 129-related updates.

The **signaling** statement is not included in this example but is discussed here for completeness. The **signaling** statement allows the router to process only the BGP\_L2VPN\_NLRIs used for BGP-based Layer 2 VPNs (FEC 128).

For interoperation scenarios in which a PE router must support both types of NLRI (FEC 128 and FEC 129), you can configure both the **signaling** statement and the **auto-discovery-only** statement. For example, a single PE router might need to process a combination of BGP-signaled virtual private wire service (VPWS) and LDP-signaled VPLS assisted by BGP autodiscovery. Configuring both the **signaling** statement and the **auto-discovery-only** statement together allows both types of signaling to run independently. The **signaling** statement is supported at the same hierarchy levels as the **auto-discovery-only** statement.

- **cluster**—Configuring a route reflector is optional for FEC 129 autodiscovered PE routers. In this example, the **cluster** statement configures Router RR to be a route reflector in the IBGP group. For inbound updates, BGP autodiscovery NLRI messages are accepted if the router is configured to be a route reflector or if the **keep all** statement is configured in the IBGP group.

- **l2vpn-id**—Specifies a globally unique Layer 2 VPN community identifier for the instance. This statement is configurable for routing instances of type **vpls**.

You can configure the following formats for the community identifier:

- Autonomous system (AS) number format—**l2vpn-id:as-number:2-byte-number**. For example: **l2vpn-id:100:200**. The AS number can be in the range from 1 through 65,535.
- IPv4 format—**l2vpn-id:ip-address:2-byte-number**. For example: **l2vpn-id:10.1.1.1:2**.
- **vrf-target**—Defines the import and export route targets for the NLRI. You must either configure the **vrf-target** statement or the **vrf-import** and **vrf-export** statements to define the instance import and export policy or the import and export route targets for the NLRI. This example uses the **vrf-target** statement.
- **route-distinguisher**—Forms part of the BGP autodiscovery NLRI and distinguishes to which VPN or VPLS routing instance each route belongs. Each route distinguisher is a 6-byte value. You must configure a unique route distinguisher for each routing instance.

You can configure the following formats for the route distinguisher:

- AS number format—**as-number:2-byte-number**
- IPv4 format—**ip-address:2-byte-number**

Two notable statements are included in this example. These statements are important for interoperability with other vendors' equipment. The interoperability statements are not necessary for the topology that is used in this example, but they are included for completeness.

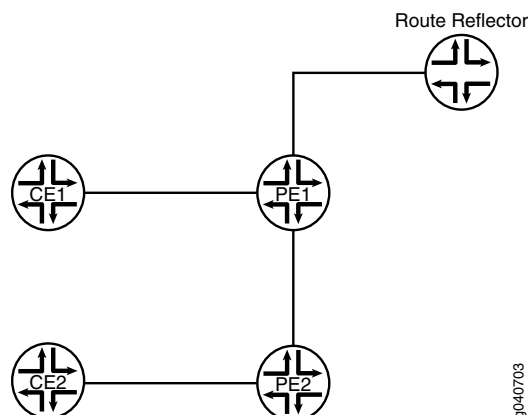
The interoperability statements are as follows:

- **input-vlan-map pop**—Removes an outer VLAN tag from the top of the VLAN tag stack.
- **output-vlan-map push**—Adds an outer VLAN tag in front of the existing VLAN tag.

### Topology Diagram

Figure 63 on page 727 shows the topology used in this example.

Figure 63: BGP Autodiscovery for LDP VPLS



## Configuration

**CLI Quick Configuration** To quickly configure BGP autodiscovery for LDP VPLS, copy the following commands, remove any line breaks, and then paste the commands into the CLI of each device.

On Router PE1:

```
[edit]
set interfaces ge-0/1/0 vlan-tagging
set interfaces ge-0/1/0 encapsulation flexible-ethernet-services
set interfaces ge-0/1/0 unit 100 encapsulation vlan-vpls
set interfaces ge-0/1/0 unit 100 vlan-id 100
set interfaces ge-0/1/0 unit 100 input-vlan-map pop
set interfaces ge-0/1/0 unit 100 output-vlan-map push
set interfaces ge-0/1/0 unit 100 family vpls
set interfaces ge-0/1/0 unit 200 encapsulation vlan-vpls
set interfaces ge-0/1/0 unit 200 vlan-id 200
set interfaces ge-0/1/0 unit 200 family vpls
set interfaces ge-0/1/1 unit 0 description "PE1 to PE2"
set interfaces ge-0/1/1 unit 0 family inet address 192.0.2.1/24
set interfaces ge-0/1/1 unit 0 family iso
set interfaces ge-0/1/1 unit 0 family mpls
set interfaces ge-0/3/0 unit 0 description "PE1 to RR"
set interfaces ge-0/3/0 unit 0 family inet address 192.0.2.2/24
set interfaces ge-0/3/0 unit 0 family iso
set interfaces ge-0/3/0 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 192.0.2.3/24
set routing-options router-id 192.0.2.3
set routing-options autonomous-system 100
set protocols mpls interface lo0.0
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols bgp group int type internal
set protocols bgp group int local-address 192.0.2.3
set protocols bgp group int family l2vpn auto-discovery-only
set protocols bgp group int neighbor 192.0.2.4
set protocols isis level 1 disable
set protocols isis interface all
set protocols isis interface fxp0.0 disable
set protocols isis interface lo0.0
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0
set routing-instances vpls100 instance-type vpls
set routing-instances vpls100 interface ge-0/1/0.100
set routing-instances vpls100 route-distinguisher 192.0.2.3:100
set routing-instances vpls100 l2vpn-id l2vpn-id:100:100
set routing-instances vpls100 vrf-target target:100:100
set routing-instances vpls100 protocols vpls no-tunnel-services
set routing-instances vpls200 instance-type vpls
set routing-instances vpls200 interface ge-0/1/0.200
set routing-instances vpls200 route-distinguisher 192.0.2.3:200
set routing-instances vpls200 l2vpn-id l2vpn-id:100:200
set routing-instances vpls200 vrf-target target:100:208
set routing-instances vpls200 protocols vpls no-tunnel-services
```

On Device CE1:

```
[edit]
set interfaces ge-1/2/1 vlan-tagging
set interfaces ge-1/2/1 mtu 1400
set interfaces ge-1/2/1 unit 100 vlan-id 100
set interfaces ge-1/2/1 unit 100 family inet address 192.0.2.5/24
set interfaces ge-1/2/1 unit 200 vlan-id 200
set interfaces ge-1/2/1 unit 200 family inet address 192.0.2.6/24
set protocols ospf area 0.0.0.0 interface ge-1/2/1.100
set protocols ospf area 0.0.0.0 interface ge-1/2/1.200
```

On Router PE2:

```
[edit]
set interfaces ge-1/1/0 vlan-tagging
set interfaces ge-1/1/0 encapsulation flexible-ethernet-services
set interfaces ge-1/1/0 unit 100 encapsulation vlan-vpls
set interfaces ge-1/1/0 unit 100 vlan-id 100
set interfaces ge-1/1/0 unit 100 input-vlan-map pop
set interfaces ge-1/1/0 unit 100 output-vlan-map push
set interfaces ge-1/1/0 unit 100 family vpls
set interfaces ge-1/1/0 unit 200 encapsulation vlan-vpls
set interfaces ge-1/1/0 unit 200 vlan-id 200
set interfaces ge-1/1/0 unit 200 family vpls
set interfaces ge-1/2/1 unit 0 description "PE2 to PE1"
set interfaces ge-1/2/1 unit 0 family inet address 192.0.2.7/24
set interfaces ge-1/2/1 unit 0 family iso
set interfaces ge-1/2/1 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 192.0.2.8/24
set routing-options router-id 192.0.2.8
set routing-options autonomous-system 100
set protocols mpls interface lo0.0
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols bgp group int type internal
set protocols bgp group int local-address 192.0.2.8
set protocols bgp group int family l2vpn auto-discovery-only
set protocols bgp group int neighbor 192.0.2.4
set protocols isis level 1 disable
set protocols isis interface ge-1/2/1.0
set protocols isis interface lo0.0
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0
set routing-instances vpls100 instance-type vpls
set routing-instances vpls100 interface ge-1/1/0.100
set routing-instances vpls100 route-distinguisher 192.0.2.8:100
set routing-instances vpls100 l2vpn-id l2vpn-id:100:100
set routing-instances vpls100 vrf-target target:100:100
set routing-instances vpls100 protocols vpls no-tunnel-services
set routing-instances vpls200 instance-type vpls
set routing-instances vpls200 interface ge-1/1/0.200
set routing-instances vpls200 route-distinguisher 192.0.2.8:200
set routing-instances vpls200 l2vpn-id l2vpn-id:100:200
set routing-instances vpls200 vrf-target target:100:208
```

```
set routing-instances vpls200 protocols vpls no-tunnel-services
```

On Device CE2:

```
[edit]
set interfaces ge-1/1/0 vlan-tagging
set interfaces ge-1/1/0 mtu 1400
set interfaces ge-1/1/0 unit 100 vlan-id 100
set interfaces ge-1/1/0 unit 100 family inet address 192.0.2.9/24
set interfaces ge-1/1/0 unit 200 vlan-id 200
set interfaces ge-1/1/0 unit 200 family inet address 192.0.2.10/24
set protocols ospf area 0.0.0.0 interface ge-1/1/0.100
set protocols ospf area 0.0.0.0 interface ge-1/1/0.200
```

On Router RR:

```
[edit]
set interfaces ge-1/3/2 unit 0 description "RR to PE1"
set interfaces ge-1/3/2 unit 0 family inet address 192.0.2.11/24
set interfaces ge-1/3/2 unit 0 family iso
set interfaces ge-1/3/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 192.0.2.4/24
set routing-options router-id 192.0.2.4
set routing-options autonomous-system 100
set protocols bgp group int type internal
set protocols bgp group int local-address 192.0.2.4
set protocols bgp group int family l2vpn auto-discovery-only
set protocols bgp group int cluster 107.107.107.107
set protocols bgp group int neighbor 192.0.2.3
set protocols bgp group int neighbor 192.0.2.8
set protocols isis level 1 disable
set protocols isis interface all
set protocols isis interface fxp0.0 disable
set protocols isis interface lo0.0
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0
```

### Router PE1

---

#### Step-by-Step Procedure

To configure Router PE1:

1. Configure the interfaces, the interface encapsulation, and the protocol families.

```
[edit]
user@PE1# edit interfaces
[edit interfaces]
user@PE1# set ge-0/1/0 encapsulation flexible-ethernet-services
user@PE1# set ge-0/1/0 unit 100 encapsulation vlan-vpls
user@PE1# set ge-0/1/0 unit 100 family vpls
user@PE1# set ge-0/1/0 unit 200 encapsulation vlan-vpls
user@PE1# set ge-0/1/0 unit 200 family vpls
user@PE1# set ge-0/1/1 unit 0 description "PE1 to PE2"
user@PE1# set ge-0/1/1 unit 0 family inet address 192.0.2.1/24
user@PE1# set ge-0/1/1 unit 0 family iso
user@PE1# set ge-0/1/1 unit 0 family mpls
user@PE1# set ge-0/3/0 unit 0 description "PE1 to RR"
```

```

user@PE1# set ge-0/3/0 unit 0 family inet address 192.0.2.2/24
user@PE1# set ge-0/3/0 unit 0 family iso
user@PE1# set ge-0/3/0 unit 0 family mpls
user@PE1# set lo0 unit 0 family inet address 192.0.2.3/24

```

2. Configure the VLANs.

```

[edit interfaces]
user@PE1# set ge-0/1/0 vlan-tagging
user@PE1# set ge-0/1/0 unit 100 vlan-id 100
user@PE1# set ge-0/1/0 unit 100 input-vlan-map pop
user@PE1# set ge-0/1/0 unit 100 output-vlan-map push
user@PE1# set ge-0/1/0 unit 200 vlan-id 200
user@PE1# exit

```

3. Configure the protocol-independent properties.

We recommend that the router ID be the same as the local address. (See the **local-address** statement in Step 4.)

```

[edit]
user@PE1# edit routing-options
[edit routing-options]
user@PE1# set router-id 192.0.2.3
user@PE1# set autonomous-system 100
user@PE1# exit

```

4. Configure IBGP, including the **auto-discovery-only** statement.

```

[edit]
user@PE1# edit protocols
[edit protocols]
user@PE1# set bgp group int type internal
user@PE1# set bgp group int local-address 192.0.2.3
user@PE1# set bgp group int family l2vpn auto-discovery-only
user@PE1# set bgp group int neighbor 192.0.2.4

```

5. Configure MPLS, LDP, and an IGP.

```

[edit protocols]
user@PE1# set mpls interface lo0.0
user@PE1# set mpls interface all
user@PE1# set mpls interface fxp0.0 disable
user@PE1# set isis level 1 disable
user@PE1# set isis interface all
user@PE1# set isis interface fxp0.0 disable
user@PE1# set isis interface lo0.0
user@PE1# set ldp interface all
user@PE1# set ldp interface fxp0.0 disable
user@PE1# set ldp interface lo0.0
user@PE1# exit

```

6. Configure the routing instances.

The **no-tunnel-services** statement is required if you are using LSI interfaces for VPLS instead of **vt** interfaces.

```

[edit]
user@PE1# edit routing-instances

```

```
[edit routing-instances]
user@PE1# set vpls100 instance-type vpls
user@PE1# set vpls100 interface ge-0/1/0.100
user@PE1# set vpls100 route-distinguisher 192.0.2.3:100
user@PE1# set vpls100 l2vpn-id l2vpn-id:100:100
user@PE1# set vpls100 vrf-target target:100:100
user@PE1# set vpls100 protocols vpls no-tunnel-services
user@PE1# set vpls200 instance-type vpls
user@PE1# set vpls200 interface ge-0/1/0.200
user@PE1# set vpls200 route-distinguisher 192.0.2.3:200
user@PE1# set vpls200 l2vpn-id l2vpn-id:100:200
user@PE1# set vpls200 vrf-target target:100:208
user@PE1# set vpls200 protocols vpls no-tunnel-services
```

7. If you are done configuring the device, commit the configuration.

```
[edit]
user@PE1# commit
```

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

```
user@PE1# show interfaces
ge-0/1/0 {
 vlan-tagging;
 encapsulation flexible-ethernet-services;
 unit 100 {
 encapsulation vlan-vpls;
 vlan-id 100;
 input-vlan-map pop;
 output-vlan-map push;
 family vpls;
 }
 unit 200 {
 encapsulation vlan-vpls;
 vlan-id 200;
 family vpls;
 }
}
ge-0/1/1 {
 unit 0 {
 description "PE1 to PE2";
 family inet {
 address 192.0.2.1/24;
 }
 family iso;
 family mpls;
 }
}
ge-0/3/0 {
 unit 0 {
 description "PE1 to RR";
 family inet {
```



```

 address 192.0.2.2/24;
 }
 family iso;
 family mpls;
}
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.3/24;
 }
 }
}

user@PE1# show protocols
mpls {
 interface lo0.0;
 interface all;
 interface fxp0 disable;
}
bgp {
 group int {
 type internal;
 local-address 192.0.2.3;
 family l2vpn {
 auto-discovery-only;
 }
 neighbor 192.0.2.4;
 }
}
isis {
 level 1 disable;
 interface all;
 interface lo0.0;
 interface fxp0 disable;
}
ldp {
 interface lo0.0;
 interface all;
 interface fxp0 disable;
}

user@PE1# show routing-options
router-id 192.0.2.3;
autonomous-system 100;

user@PE1# show routing-instances
vpls100 {
 instance-type vpls;
 interface ge-0/1/0.100;
 route-distinguisher 192.0.2.3:100;
 l2vpn-id l2vpn-id:100:100;
 vrf-target target:100:100;
 protocols {
 vpls {
 no-tunnel-services;
 }
 }
}

```

```
 }
 }
 vpls200 {
 instance-type vpls;
 interface ge-0/1/0.200;
 route-distinguisher 192.0.2.3:200;
 l2vpn-id l2vpn-id:100:200;
 vrf-target target:100:208;
 protocols {
 vpls {
 no-tunnel-services;
 }
 }
 }
}
```

---

### Device CE1

#### Step-by-Step Procedure

To configure Device CE1:

1. Configure interface addresses and the interface maximum transmission unit (MTU).

```
[edit]
user@CE1# edit interfaces
[edit interfaces]
user@CE1# set ge-1/2/1 mtu 1400
user@CE1# set ge-1/2/1 unit 100 family inet address 192.0.2.5/24
user@CE1# set ge-1/2/1 unit 200 family inet address 192.0.2.6/24
```

2. Configure VLANs.

```
[edit interfaces]
user@CE1# set ge-1/2/1 vlan-tagging
user@CE1# set ge-1/2/1 unit 100 vlan-id 100
user@CE1# set ge-1/2/1 unit 200 vlan-id 200
user@CE1# exit
```

3. Configure an IGP.

```
user@CE1# edit protocols
[edit protocols]
user@CE1# set ospf area 0.0.0.0 interface ge-1/2/1.100
user@CE1# set ospf area 0.0.0.0 interface ge-1/2/1.200
user@CE1# exit
```

4. If you are done configuring the device, commit the configuration.

```
[edit]
user@CE1# commit
```

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

```
user@CE1# show interfaces
ge-1/2/1 {
 vlan-tagging;
 mtu 1400;
```

```

unit 100 {
 vlan-id 100;
 family inet {
 address 192.0.2.5/24;
 }
}
unit 200 {
 vlan-id 200;
 family inet {
 address 192.0.2.6/24;
 }
}
}

user@CE1# show protocols
ospf {
 area 0.0.0.0 {
 interface ge-1/2/1.100;
 interface ge-1/2/1.200;
 }
}

```

### Router PE2

#### Step-by-Step Procedure

To configure Router PE2:

1. Configure the interfaces, the interface encapsulation, and the protocol families.

```

[edit]
user@PE2# edit interfaces
[edit interfaces]
user@PE2# set ge-1/1/0 encapsulation flexible-ethernet-services
user@PE2# set ge-1/1/0 unit 100 encapsulation vlan-vpls
user@PE2# set ge-1/1/0 unit 100 family vpls
user@PE2# set ge-1/1/0 unit 200 encapsulation vlan-vpls
user@PE2# set ge-1/1/0 unit 200 family vpls
user@PE2# set ge-1/2/1 unit 0 description "PE2 to PE1"
user@PE2# set ge-1/2/1 unit 0 family inet address 192.0.2.7/24
user@PE2# set ge-1/2/1 unit 0 family iso
user@PE2# set ge-1/2/1 unit 0 family mpls
user@PE2# set lo0 unit 0 family inet address 192.0.2.8/24

```

2. Configure the VLANs.

```

[edit interfaces]
user@PE2# set ge-1/1/0 vlan-tagging
user@PE2# set ge-1/1/0 unit 100 vlan-id 100
user@PE2# set ge-1/1/0 unit 100 input-vlan-map pop
user@PE2# set ge-1/1/0 unit 100 output-vlan-map push
user@PE2# set ge-1/1/0 unit 200 vlan-id 200
user@PE2# exit

```

3. Configure the protocols-independent properties.

We recommend that the router ID be the same as the local address. (See the **local-address** statement in Step 4.)

```

[edit]

```

```
user@PE2# edit routing-options
[edit routing-options]
user@PE2# set router-id 192.0.2.8
user@PE2# set autonomous-system 100
```

4. Configure IBGP, including the **auto-discovery-only** statement.

```
[edit]
user@PE2# edit protocols
[edit protocols]
user@PE2# set bgp group int type internal
user@PE2# set bgp group int local-address 192.0.2.8
user@PE2# set bgp group int family l2vpn auto-discovery-only
user@PE2# set bgp group int neighbor 192.0.2.4
```

5. Configure MPLS, LDP, and an IGP.

```
[edit protocols]
user@PE2# set mpls interface lo0.0
user@PE2# set mpls interface all
user@PE2# set mpls interface fxp0.0 disable
user@PE2# set isis level 1 disable
user@PE2# set isis interface ge-1/2/1.0
user@PE2# set isis interface lo0.0
user@PE2# set ldp interface all
user@PE2# set ldp interface fxp0.0 disable
user@PE2# set ldp interface lo0.0
user@PE2# exit
```

6. Configure the routing instances.

The **no-tunnel-services** statement is required if you are using LSI interfaces for VPLS instead of **vt** interfaces.

```
[edit]
user@PE2# edit routing-instances
[edit routing-instances]
user@PE2# set vpls100 instance-type vpls
user@PE2# set vpls100 interface ge-1/1/0.100
user@PE2# set vpls100 route-distinguisher 192.0.2.8:100
user@PE2# set vpls100 l2vpn-id l2vpn-id:100:100
user@PE2# set vpls100 vrf-target target:100:100
user@PE2# set vpls100 protocols vpls no-tunnel-services
user@PE2# set vpls200 instance-type vpls
user@PE2# set vpls200 interface ge-1/1/0.200
user@PE2# set vpls200 route-distinguisher 192.0.2.8:200
user@PE2# set vpls200 l2vpn-id l2vpn-id:100:200
user@PE2# set vpls200 vrf-target target:100:208
user@PE2# set vpls200 protocols vpls no-tunnel-services
```

7. If you are done configuring the device, commit the configuration.

```
[edit]
user@PE2# commit
```

**Results** From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols**, **show routing-options**, and **show routing-instances** commands. If the

output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```

user@PE2# show interfaces
ge-1/1/0 {
 vlan-tagging;
 encapsulation flexible-ethernet-services;
 unit 100 {
 encapsulation vlan-vpls;
 vlan-id 100;
 input-vlan-map pop;
 output-vlan-map push;
 family vpls;
 }
 unit 200 {
 encapsulation vlan-vpls;
 vlan-id 200;
 family vpls;
 }
}
ge-1/2/1 {
 unit 0 {
 description "PE2 to PE1";
 family inet {
 address 192.0.2.7/24;
 }
 family iso;
 family mpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.8/24;
 }
 }
}

user@PE2# show protocols
mpls {
 interface lo0.0;
 interface all;
 interface fxp0 disable;
}
bgp {
 group int {
 type internal;
 local-address 192.0.2.8;
 family l2vpn {
 auto-discovery-only;
 }
 neighbor 192.0.2.4;
 }
}
isis {
 level 1 disable;
}

```

```
interface ge-1/2/1.0;
interface lo0.0;
}
ldp {
 interface lo0.0;
 interface all;
 interface fxp0 disable;
}

user@PE2# show routing-options
router-id 192.0.2.8;
autonomous-system 100;

user@PE2# show routing-instances
vpls100 {
 instance-type vpls;
 interface ge-1/1/0.100;
 route-distinguisher 192.0.2.8:100;
 l2vpn-id l2vpn-id:100:100;
 vrf-target target:100:100;
 protocols {
 vpls {
 no-tunnel-services;
 }
 }
}
vpls200 {
 instance-type vpls;
 interface ge-1/1/0.200;
 route-distinguisher 192.0.2.8:200;
 l2vpn-id l2vpn-id:100:200;
 vrf-target target:100:208;
 protocols {
 vpls {
 no-tunnel-services;
 }
 }
}
```

---

### Device CE2

#### Step-by-Step Procedure

To configure Device CE2:

1. Configure VLAN interfaces.

```
[edit]
user@CE2# edit interfaces ge-1/1/0
[edit interfaces ge-1/1/0]
user@CE2# set vlan-tagging
user@CE2# set mtu 1400
user@CE2# set unit 100 vlan-id 100
user@CE2# set unit 100 family inet address 192.0.2.9/24
user@CE2# set unit 200 vlan-id 200
user@CE2# set unit 200 family inet address 192.0.2.10/24
user@CE2# exit
```

2. Configure OSPF on the interfaces.

```
[edit]
user@CE2# edit protocols ospf area 0.0.0.0
[edit protocols ospf area 0.0.0.0]
user@CE2# set interface ge-1/1/0.100
user@CE2# set interface ge-1/1/0.200
user@CE2# exit
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@CE2# commit
```

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

```
user@CE2# show interfaces
ge-1/1/0 {
 vlan-tagging;
 mtu 1400;
 unit 100 {
 vlan-id 100;
 family inet {
 address 192.0.2.9/24;
 }
 }
 unit 200 {
 vlan-id 200;
 family inet {
 address 192.0.2.10/24;
 }
 }
}

user@CE2# show protocols
ospf {
 area 0.0.0.0 {
 interface ge-1/1/0.100;
 interface ge-1/1/0.200;
 }
}
```

## Router RR

**Step-by-Step Procedure** To configure Router RR:

1. Configure interface addresses and the protocol families.

```
[edit]
user@RR# edit interfaces
[edit interfaces]
user@RR# set ge-1/3/2 unit 0 description "RR to PE1"
user@RR# set ge-1/3/2 unit 0 family inet address 192.0.2.11/24
user@RR# set ge-1/3/2 unit 0 family iso
```

```
user@RR# set ge-1/3/2 unit 0 family mpls
user@RR# set lo0 unit 0 family inet address 192.0.2.4/32
user@RR# exit
```

2. Configure the autonomous systems and the router ID.

```
[edit]
user@RR# edit routing-options
[edit routing-options]
user@RR# set autonomous-system 100
user@RR# set router-id 192.0.2.4
user@RR# exit
```

3. Configure BGP and set this router to be the route reflector. Route reflection is optional for FEC 129.

```
[edit]
user@RR# edit protocols bgp group int
[edit protocols bgp group int]
user@RR# set type internal
user@RR# set local-address 192.0.2.4
user@RR# set family l2vpn auto-discovery-only
user@RR# set cluster 107.107.107.107
user@RR# set neighbor 192.0.2.3
user@RR# set neighbor 192.0.2.8
user@RR# exit
```

4. Configure IS-IS for the IGP.

```
[edit]
user@RR# edit protocols isis
[edit protocols isis]
user@RR# set level 1 disable
user@RR# set interface all
user@RR# set interface fxp0.0 disable
user@RR# set interface lo0.0
user@RR# exit
```

5. Configure LDP for the MPLS signaling protocol.

```
[edit]
user@RR# edit protocols ldp
[edit protocols ldp]
user@RR# set interface all
user@RR# set interface fxp0.0 disable
user@RR# set interface lo0.0
user@RR# exit
```

6. If you are done configuring the device, commit the configuration.

```
[edit]
user@RR# commit
```

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

```
user@RR# show interfaces
```



```

ge-1/3/2 {
 unit 0 {
 description "RR to PE1";
 family inet {
 address 192.0.2.11/24;
 }
 family iso;
 family mpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.4/32;
 }
 }
}

user@RR# show protocols
bgp {
 group int {
 type internal;
 local-address 192.0.2.4;
 family l2vpn {
 auto-discovery-only;
 }
 cluster 107.107.107.107;
 neighbor 192.0.2.3;
 neighbor 192.0.2.8;
 }
}
isis {
 level 1 disable;
 interface lo0.0;
 interface all;
 interface fxp0 disable;
}
ldp {
 interface lo0.0;
 interface all;
 interface fxp0 disable;
}

user@RR# show routing-options
router-id 192.0.2.4;
autonomous-system 100;

```

## Verification

To verify the operation, use the following commands:

- `show route extensive`
- `show route advertising-protocol bgp neighbor`
- `show route receive-protocol bgp neighbor`

- `show route table bgp.l2vpn.0`
- `show route table vpls100.l2vpn.0`
- `show route table vpls200.l2vpn.0`
- [show vpls connections](#) extensive
- [show vpls mac-table](#) detail
- [show vpls statistics](#)

AD in the routing table output indicates autodiscovery NLRI.

**Related  
Documentation**

- [Example: Configuring BGP Autodiscovery for LDP VPLS with User-Defined Mesh Groups on page 742](#)
- [Configuring Interoperability Between BGP Signaling and LDP Signaling in VPLS on page 556](#)

## [Example: Configuring BGP Autodiscovery for LDP VPLS with User-Defined Mesh Groups](#)

This example describes how to configure user-defined mesh groups for BGP autodiscovery for LDP VPLS, as specified in forwarding equivalency class (FEC) 129. FEC 129 uses BGP autodiscovery to convey endpoint information, so you do not need to manually configure pseudowires. You configure mesh groups on the border router to group the sets of PE routers that are automatically fully meshed and that share the same signaling protocol, either BGP or LDP. You can configure multiple mesh groups to map each fully meshed LDP-signaled or BGP-signaled VPLS domain to a mesh group.

- [Requirements on page 742](#)
- [Overview on page 742](#)
- [Configuration on page 743](#)
- [Verification on page 748](#)

### Requirements

Before you begin, configure BGP autodiscovery for LDP VPLS. See [“Example: Configuring BGP Autodiscovery for LDP VPLS” on page 725](#).

The hardware and software requirements for this example are the same as the requirements for the *Example: Configuring BGP Autodiscovery for LDP VPLS*. You will need to adapt the example configuration to the topology used in this example.

### Overview

Configuration for a mesh group for FEC 129 is very similar to the mesh-group configuration for FEC 128.

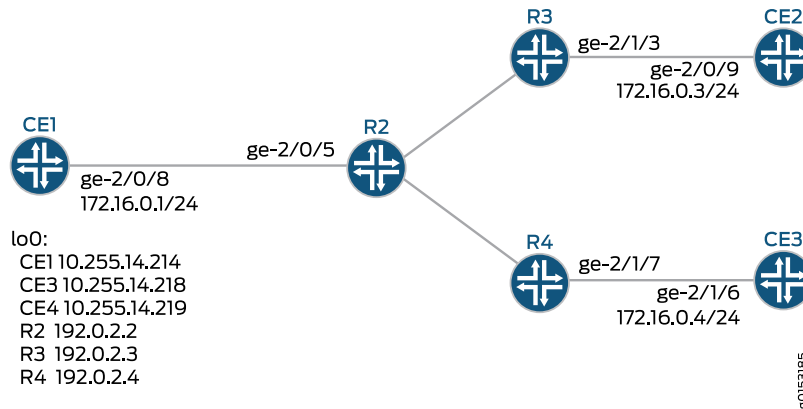
Note the following differences for FEC 129:

- Each user-defined mesh group must have a unique route distinguisher. Do not use the route distinguisher that is defined for the default mesh group at the **[edit routing-instances]** hierarchy level.
- Each user-defined mesh group must have its own import and export route target.
- Each user-defined mesh group can have a unique Layer 2 VPN ID. By default, all the mesh groups that are configured for a VPLS routing instance use the same Layer 2 VPN ID as the one that you configure at the **[edit routing-instances]** hierarchy level.

### Topology Diagram

Figure 64 on page 743 shows a topology that includes a user-defined mesh group.

**Figure 64: BGP Autodiscovery for LDP VPLS with a User-Defined Mesh Group**



“CLI Quick Configuration” on page 743 shows the configuration for all of the devices in Figure 64 on page 743. The section “Step-by-Step Procedure” on page 745 describes the steps on Device R2.

### Configuration

|                                |                                                                                                                                                                                                                       |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CLI Quick Configuration</b> | To quickly configure a mesh group, copy the following commands, remove any line breaks, and then paste the commands into the CLI of each device.                                                                      |
| <b>Device CE1</b>              | <pre>set interfaces ge-2/0/8 unit 0 set interfaces lo0 unit 0 family inet address 10.255.14.214/32 set protocols ospf area 0.0.0.0 interface lo0.0 passive set protocols ospf area 0.0.0.0 interface ge-2/0/8.0</pre> |
| <b>Device CE3</b>              | <pre>set interfaces ge-2/0/9 unit 0 set interfaces lo0 unit 0 family inet address 10.255.14.218/32 set protocols ospf area 0.0.0.0 interface lo0.0 passive set protocols ospf area 0.0.0.0 interface ge-2/0/9.0</pre> |
| <b>Device CE4</b>              | <pre>set interfaces ge-2/1/6 unit 0 set interfaces lo0 unit 0 family inet address 10.255.14.219/32</pre>                                                                                                              |

```
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface ge-2/1/6.0
```

```
Device R2 set interfaces ge-2/0/5 encapsulation ethernet-vpls
 set interfaces ge-2/0/5 unit 0 description to_CE1
 set interfaces ge-2/0/5 unit 0 family vpls
 set interfaces ge-2/0/10 unit 0 description to_R3
 set interfaces ge-2/0/10 unit 0 family inet address 10.10.4.2/30
 set interfaces ge-2/0/10 unit 0 family mpls
 set interfaces ge-2/0/11 unit 0 description to_R4
 set interfaces ge-2/0/11 unit 0 family inet address 10.10.5.1/30
 set interfaces ge-2/0/11 unit 0 family mpls
 set interfaces lo0 unit 0 family inet address 192.0.2.2/24
 set protocols mpls interface ge-2/0/10.0
 set protocols mpls interface ge-2/0/11.0
 set protocols bgp local-address 192.0.2.2
 set protocols bgp group pe-pe type internal
 set protocols bgp group pe-pe connect-retry-interval 1
 set protocols bgp group pe-pe family l2vpn auto-discovery-only
 set protocols bgp group pe-pe family l2vpn signaling
 set protocols bgp group pe-pe neighbor 192.0.2.3
 set protocols bgp group pe-pe neighbor 192.0.2.4
 set protocols ospf traffic-engineering
 set protocols ospf area 0.0.0.0 interface lo0.0 passive
 set protocols ospf area 0.0.0.0 interface ge-2/0/10.0
 set protocols ospf area 0.0.0.0 interface ge-2/0/11.0
 set protocols ldp interface ge-2/0/10.0
 set protocols ldp interface ge-2/0/11.0
 set protocols ldp interface lo0.0
 set routing-instances inst512 instance-type vpls
 set routing-instances inst512 interface ge-2/0/5.0
 set routing-instances inst512 route-distinguisher 100:100
 set routing-instances inst512 l2vpn-id l2vpn-id:1:2
 set routing-instances inst512 vrf-target target:1:1
 set routing-instances inst512 protocols vpls mesh-group metro1 vrf-target target:2:1
 set routing-instances inst512 protocols vpls mesh-group metro1 route-distinguisher
 100:200
 set routing-options autonomous-system 64510
```

```
Device R3 set interfaces ge-2/0/10 unit 0 description to_R2
 set interfaces ge-2/0/10 unit 0 family inet address 10.10.4.1/30
 set interfaces ge-2/0/10 unit 0 family mpls
 set interfaces ge-2/1/3 encapsulation ethernet-vpls
 set interfaces ge-2/1/3 unit 0 description to_CE3
 set interfaces ge-2/1/3 unit 0 family vpls
 set interfaces lo0 unit 0 family inet address 192.0.2.3/24
 set protocols mpls interface ge-2/0/10.0
 set protocols bgp local-address 192.0.2.3
 set protocols bgp group pe-pe type internal
 set protocols bgp group pe-pe connect-retry-interval 1
 set protocols bgp group pe-pe family l2vpn auto-discovery-only
 set protocols bgp group pe-pe family l2vpn signaling
 set protocols bgp group pe-pe neighbor 192.0.2.2
 set protocols bgp group pe-pe neighbor 192.0.2.4
 set protocols ospf traffic-engineering
```

```

set protocols ospf area 0.0.0.0 interface ge-2/0/10.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ldp interface ge-2/0/10.0
set protocols ldp interface lo0.0
set routing-instances inst512 instance-type vpls
set routing-instances inst512 interface ge-2/1/3.0
set routing-instances inst512 route-distinguisher 100:100
set routing-instances inst512 l2vpn-id l2vpn-id:1:2
set routing-instances inst512 vrf-target target:1:1
set routing-instances inst512 protocols vpls
set routing-options autonomous-system 64510

```

**Device R4**

```

set interfaces ge-2/0/10 unit 0 description to_R2
set interfaces ge-2/0/10 unit 0 family inet address 10.10.5.2/30
set interfaces ge-2/0/10 unit 0 family mpls
set interfaces ge-2/1/7 encapsulation ethernet-vpls
set interfaces ge-2/1/7 unit 0 description to_CE4
set interfaces ge-2/1/7 unit 0 family vpls
set interfaces lo0 unit 0 family inet address 192.0.2.4/24
set protocols mpls interface ge-2/0/10.0
set protocols bgp local-address 192.0.2.4
set protocols bgp group pe-pe type internal
set protocols bgp group pe-pe connect-retry-interval 1
set protocols bgp group pe-pe family l2vpn auto-discovery-only
set protocols bgp group pe-pe family l2vpn signaling
set protocols bgp group pe-pe neighbor 192.0.2.2
set protocols bgp group pe-pe neighbor 192.0.2.3
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface ge-2/0/10.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ldp interface ge-2/0/10.0
set protocols ldp interface lo0.0
set routing-instances inst512 instance-type vpls
set routing-instances inst512 interface ge-2/1/7.0
set routing-instances inst512 route-distinguisher 100:100
set routing-instances inst512 l2vpn-id l2vpn-id:1:2
set routing-instances inst512 vrf-target target:1:1
set routing-instances inst512 protocols vpls
set routing-options autonomous-system 64510

```

**Step-by-Step Procedure** To configure a mesh group:

1. Configure the interfaces.

```

[edit interfaces]
user@R2# set ge-2/0/5 encapsulation ethernet-vpls
user@R2# set ge-2/0/5 unit 0 description to_CE1
user@R2# set ge-2/0/5 unit 0 family vpls

user@R2# set ge-2/0/10 unit 0 description to_R3
user@R2# set ge-2/0/10 unit 0 family inet address 10.10.4.2/30
user@R2# set ge-2/0/10 unit 0 family mpls

user@R2# set ge-2/0/11 unit 0 description to_R4
user@R2# set ge-2/0/11 unit 0 family inet address 10.10.5.1/30

```

```
user@R2# set ge-2/0/11 unit 0 family mpls
```

```
user@R2# set lo0 unit 0 family inet address 192.0.2.2/24
```

2. Configure MPLS on the interfaces.

```
[edit protocols mpls]
user@R2# set interface ge-2/0/10.0
user@R2# set interface ge-2/0/11.0
```

3. Configure BGP.

```
[edit protocols bgp]
user@R2# set local-address 192.0.2.2
```

```
[edit protocols bgp group pe-pe]
user@R2# set type internal
user@R2# set connect-retry-interval 1
user@R2# set family l2vpn auto-discovery-only
user@R2# set family l2vpn signaling
user@R2# set neighbor 192.0.2.3
user@R2# set neighbor 192.0.2.4
```

4. Set the import and export route target for the default mesh group.

```
[edit protocols ospf]
user@R2# set traffic-engineering
user@R2# set area 0.0.0.0 interface lo0.0 passive
user@R2# set area 0.0.0.0 interface ge-2/0/10.0
user@R2# set area 0.0.0.0 interface ge-2/0/11.0
```

5. Configure LDP on the core-facing interfaces and on the loopback interface.

```
[edit protocols ldp]
user@R2# set interface ge-2/0/10.0
user@R2# set interface ge-2/0/11.0
user@R2# set interface lo0.0
```

6. Configure the VPLS routing instance.

Make sure that the route distinguisher in the mesh group is unique.

```
[edit routing-instances inst512]
user@R2# set instance-type vpls
user@R2# set interface ge-2/0/5.0
user@R2# set route-distinguisher 100:100
user@R2# set l2vpn-id l2vpn-id:1:2
user@R2# set vrf-target target:1:1
user@R2# set protocols vpls mesh-group metro1 vrf-target target:2:1
user@R2# set protocols vpls mesh-group metro1 route-distinguisher 100:200
```

7. Configure the autonomous system (AS) number.

```
[edit routing-options]
user@R2# set autonomous-system 64510
```

8. If you are done configuring the device, commit the configuration.

```
[edit]
```

```
user@R2# commit
```

**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@R2# show interfaces
ge-2/0/5 {
 encapsulation ethernet-vpls;
 unit 0 {
 description PE1_to_CE1;
 family vpls;
 }
}
ge-2/0/10 {
 unit 0 {
 description to_R3;
 family inet {
 address 10.10.4.2/30;
 }
 family mpls;
 }
}
ge-2/0/11 {
 unit 0 {
 description to_R4;
 family inet {
 address 10.10.5.1/30;
 }
 family mpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.2/24;
 }
 }
}

user@R2# show protocols
mpls {
 interface ge-2/0/10.0;
 interface ge-2/0/11.0;
}
bgp {
 local-address 192.0.2.2;
 group pe-pe {
 type internal;
 connect-retry-interval 1;
 family l2vpn {
 auto-discovery-only;
 signaling;
 }
 }
 neighbor 192.0.2.3;
```

```
 neighbor 192.0.2.4;
 }
}
ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface lo0.0 {
 passive;
 }
 interface ge-2/0/10.0;
 interface ge-2/0/11.0;
 }
}
ldp {
 interface ge-2/0/10.0;
 interface ge-2/0/11.0;
 interface lo0.0;
}

user@R2# show routing-instances
inst512 {
 instance-type vpls;
 interface ge-2/0/5.0;
 route-distinguisher 100:100;
 l2vpn-id l2vpn-id:1:2;
 vrf-target target:1:1;
 protocols {
 vpls {
 mesh-group metro1 {
 vrf-target target:2:1;
 route-distinguisher 100:200;
 }
 }
 }
}

user@R2# show routing-options
autonomous-system 64510;
```

## Verification

Confirm that the configuration is working properly.

- [Verifying the Routes on page 748](#)
- [Checking Connectivity on page 750](#)
- [Checking the VPLS Connections on page 751](#)
- [Display Learned VPLS MAC Address Information on page 751](#)

---

### Verifying the Routes

**Purpose** Verify that the expected routes are learned.

**Action** From operational mode, enter the **show route** command.

```
user@R2> show route
```



```
inet.0: 9 destinations, 9 routes (9 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
```

```
192.0.2.2/24 *[Direct/0] 4d 02:42:47
 > via lo0.0
192.0.2.3/24 *[OSPF/10] 4d 02:41:56, metric 1
 > to 10.10.4.1 via ge-2/0/10.0
192.0.2.4/24 *[OSPF/10] 4d 02:42:01, metric 1
 > to 10.10.5.2 via ge-2/0/11.0
10.10.3.2/24 *[Local/0] 4d 02:42:47
 Reject
10.10.4.0/30 *[Direct/0] 4d 02:42:46
 > via ge-2/0/10.0
10.10.4.2/32 *[Local/0] 4d 02:42:47
 Local via ge-2/0/10.0
10.10.5.0/30 *[Direct/0] 4d 02:42:46
 > via ge-2/0/11.0
10.10.5.1/32 *[Local/0] 4d 02:42:47
 Local via ge-2/0/11.0
203.0.113.0/24 *[OSPF/10] 4d 02:42:49, metric 1
 MultiRecv
```

```
inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
```

```
192.0.2.3/24 *[LDP/9] 4d 02:01:06, metric 1
 > to 10.10.4.1 via ge-2/0/10.0
192.0.2.4/24 *[LDP/9] 4d 02:01:06, metric 1
 > to 10.10.5.2 via ge-2/0/11.0
```

```
mpls.0: 12 destinations, 12 routes (12 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
```

```
0 *[MPLS/0] 4d 02:42:49, metric 1
 Receive
1 *[MPLS/0] 4d 02:42:49, metric 1
 Receive
2 *[MPLS/0] 4d 02:42:49, metric 1
 Receive
13 *[MPLS/0] 4d 02:42:49, metric 1
 Receive
299776 *[LDP/9] 4d 02:01:06, metric 1
 > to 10.10.5.2 via ge-2/0/11.0, Pop
299776(S=0) *[LDP/9] 4d 02:01:06, metric 1
 > to 10.10.5.2 via ge-2/0/11.0, Pop
299792 *[LDP/9] 4d 02:01:06, metric 1
 > to 10.10.4.1 via ge-2/0/10.0, Pop
299792(S=0) *[LDP/9] 4d 02:01:06, metric 1
 > to 10.10.4.1 via ge-2/0/10.0, Pop
800000 *[VPLS/7] 4d 02:01:05
 > via vt-2/0/10.185597952, Pop
800001 *[VPLS/7] 4d 02:01:05
 > via vt-2/0/10.185597953, Pop
vt-2/0/10.185597953*[VPLS/7] 4d 02:01:05, metric2 1
 > to 10.10.5.2 via ge-2/0/11.0, Push 800001
vt-2/0/10.185597952*[VPLS/7] 4d 02:01:05, metric2 1
 > to 10.10.4.1 via ge-2/0/10.0, Push 800001
```

```
bgp.12vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
```

```

100:100:192.0.2.3/96 AD
 *[BGP/170] 4d 02:32:41, localpref 100, from 192.0.2.3
 AS path: I, validation-state: unverified
 > to 10.10.4.1 via ge-2/0/10.0
100:100:192.0.2.4/96 AD
 *[BGP/170] 4d 02:32:41, localpref 100, from 192.0.2.4
 AS path: I, validation-state: unverified
 > to 10.10.5.2 via ge-2/0/11.0

inst512.12vpn.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

100:100:192.0.2.2/96 AD
 *[VPLS/170] 4d 02:01:05, metric2 1
 Indirect
100:100:192.0.2.3/96 AD
 *[BGP/170] 4d 02:32:41, localpref 100, from 192.0.2.3
 AS path: I, validation-state: unverified
 > to 10.10.4.1 via ge-2/0/10.0
100:100:192.0.2.4/96 AD
 *[BGP/170] 4d 02:32:41, localpref 100, from 192.0.2.4
 AS path: I, validation-state: unverified
 > to 10.10.5.2 via ge-2/0/11.0
100:200:192.0.2.2/96 AD
 *[VPLS/170] 4d 02:01:05, metric2 1
 Indirect
192.0.2.3:NoCtrlWord:5:1:2:192.0.2.2:192.0.2.3/176
 *[VPLS/7] 4d 02:01:05, metric2 1
 > to 10.10.4.1 via ge-2/0/10.0
192.0.2.3:NoCtrlWord:5:1:2:192.0.2.3:192.0.2.2/176
 *[LDP/9] 4d 02:01:05
 Discard
192.0.2.4:NoCtrlWord:5:1:2:192.0.2.2:192.0.2.4/176
 *[VPLS/7] 4d 02:01:05, metric2 1
 > to 10.10.5.2 via ge-2/0/11.0
192.0.2.4:NoCtrlWord:5:1:2:192.0.2.4:192.0.2.2/176
 *[LDP/9] 4d 02:01:05
 Discard

ldp.12vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.3:NoCtrlWord:5:1:2:192.0.2.3:192.0.2.2/176
 *[LDP/9] 4d 02:01:05
 Discard
192.0.2.4:NoCtrlWord:5:1:2:192.0.2.4:192.0.2.2/176
 *[LDP/9] 4d 02:01:05
 Discard

```

**Meaning** The output shows all the learned routes, including the autodiscovered (AD) routes.

### Checking Connectivity

**Purpose** Verify that Device CE1 can ping Device CE3 and Device CE4.

**Action** user@CE1> ping 10.255.14.218  
 PING 10.255.14.218 (10.255.14.218): 56 data bytes  
 64 bytes from 10.255.14.218: icmp\_seq=0 ttl=64 time=0.787 ms  
 64 bytes from 10.255.14.218: icmp\_seq=1 ttl=64 time=0.651 ms  
 ^C  
 --- 10.255.14.218 ping statistics ---  
 2 packets transmitted, 2 packets received, 0% packet loss  
 round-trip min/avg/max/stddev = 0.651/0.719/0.787/0.068 ms

user@CE1> ping 10.255.14.219  
 PING 10.255.14.219 (10.255.14.219): 56 data bytes  
 64 bytes from 10.255.14.219: icmp\_seq=0 ttl=64 time=1.054 ms  
 64 bytes from 10.255.14.219: icmp\_seq=1 ttl=64 time=0.669 ms  
 ^C  
 --- 10.255.14.219 ping statistics ---  
 2 packets transmitted, 2 packets received, 0% packet loss  
 round-trip min/avg/max/stddev = 0.669/0.862/1.054/0.193 ms

**Meaning** The output shows that VPLS is operational.

### Checking the VPLS Connections

**Purpose** Make sure that all of the FEC 129 VPLS connections come up correctly.

**Action** user@R2> show vpls connections

```
Instance: inst512
 L2vpn-id: 1:2
 Local-id: 192.0.2.2
 Mesh-group connections: __ves__
 Remote-id Type St Time last up # Up trans
 192.0.2.4 rmt Up Oct 26 15:11:56 2012 1
 Remote PE: 192.0.2.4, Negotiated control-word: No
 Incoming label: 800001, Outgoing label: 800001
 Local interface: vt-2/0/10.185597953, Status: Up, Encapsulation: ETHERNET
 Description: Intf - vpls inst512 local-id 192.0.2.2 remote-id 192.0.2.4
 neighbor 192.0.2.4
 192.0.2.3 rmt Up Oct 26 15:11:56 2012 1
 Remote PE: 192.0.2.3, Negotiated control-word: No
 Incoming label: 800000, Outgoing label: 800001
 Local interface: vt-2/0/10.185597952, Status: Up, Encapsulation: ETHERNET
 Description: Intf - vpls inst512 local-id 192.0.2.2 remote-id 192.0.2.3
 neighbor 192.0.2.3
```

**Meaning** As expected, the connections are up.

### Display Learned VPLS MAC Address Information

**Purpose** Verify that all CE devices' MAC addresses are learned and installed.

**Action** user@R2> [show vpls mac-table](#)

MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC  
SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

```
Logical system : R2
Routing instance : inst512
Bridging domain : __inst512__, VLAN : NA
 MAC MAC Logical NH RTR
 address flags interface Index ID
00:21:59:0f:35:32 D ge-2/0/5.0
00:21:59:0f:35:33 D vt-2/0/10.185597952
00:21:59:0f:35:d5 D vt-2/0/10.185597953
```

- Related Documentation**
- [Example: Configuring BGP Autodiscovery for LDP VPLS on page 725](#)
  - [Configuring Interoperability Between BGP Signaling and LDP Signaling in VPLS on page 556](#)

## VPLS Multihoming Reactions to Network Failures

VPLS multihoming is designed to protect customer sites from a loss of network connectivity in the event of the following types of network failures:

- Link failure between the CE device and the PE router—BGP on the PE router is notified when the link goes down. BGP sets the circuit status vector bit in the MP\_REACH\_NLRI to indicate that the circuit is down.

If all of the VPLS local attachment circuits are down, then BGP modifies the down bit in the VPLS advertisement Layer2-Extended-Community to indicate that the customer site is down. When the bit is modified, BGP advertises the route to all of the remote PE routers to notify them that the circuit (and site) is down. Each of the remote PE routers run the BGP and VPLS path selection procedures again and reroute the VPLS pseudowires as needed.

- MPLS connectivity failure to the remote PE router—On the multihomed PE router, BGP discovers that MPLS cannot connect to the BGP next hop in the service provider's network. BGP modifies the circuit status vector bit in the MP\_REACH\_NLRI to indicate that the LSP is down. Once the bit is modified, BGP readvertises the route to all of the remote PE routers to notify them that connectivity from the local site to the remote site is down.

The remote PE routers each run the BGP and VPLS path selection procedures again. With the LSP to the original multihomed PE router down, the remote PE routers designate the backup multihomed PE router as the VE device for the multihomed customer site. The pseudowires to and from the remote PE routers are then rerouted to the backup multihomed PE router.

- PE router failure—When either the multihomed PE router or the BGP process running on it fails, the remote PE routers detect the expiration of the holdtimer, bring down their peering sessions, and delete the Layer 2 advertisements from that multihomed PE router. The remote PE routers each run the BGP and VPLS path selection procedures again and reroute their pseudowires to the backup multihomed PE router.

Alternatively, the remote PE routers could discover that the BGP next hop, represented by the failed multihomed PE router, is unreachable. For this case, the remote PE routers mark the Layer 2 routes advertised by the multihomed PE router as unreachable. The remote PE routers each run the BGP and VPLS path selection procedures again and reroute their pseudowires to the backup multihomed PE router.

The remote PE routers behave in the same manner if you reconfigure the local preference attribute of the primary multihomed PE router (effectively performing an administrative failover to the backup multihomed PE router). On the primary multihomed PE router, BGP advertises a Layer 2 update with the new local preference attribute to all of the remote PE routers. The remote PE routers each run the BGP and VPLS path selection procedures again and reroute their pseudowires to the backup multihomed PE router.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

## Configuring VPLS Multihoming (FEC 128)

VPLS multihoming allows you to connect a customer site to multiple PE routers to provide redundant connectivity while preventing the formation of Layer 2 loops in the service provider's network. A VPLS site multihomed to two or more PE routers provides redundant connectivity in the event of a PE router-to-CE device link failure or the failure of a PE router. For more information about VPLS multihoming, see [“VPLS Multihoming Overview” on page 705](#).



**NOTE:** If you want to enable multihoming for a VPLS routing instance, you cannot also enable LDP signaling. You can only enable BGP signaling.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

The following sections describe how to configure VPLS multihoming. Some information is also provided on single-homed site configuration versus multihomed site configuration.

- [VPLS Multihomed Site Configuration on page 753](#)
- [VPLS Single-Homed Site Configuration on page 755](#)

### VPLS Multihomed Site Configuration

The following describes the requirements for a VPLS multihomed site configuration:

- Assign the same site ID on all PE routers connected to the same CE devices.
- Assign unique route distinguishers for each multihomed PE router.

- Reference all interfaces assigned to the multihomed VPLS site on each PE router. Only one of these interfaces is used to send and receive traffic for this site at a time.
- Either designate a primary interface or allow the router to select the interface to be used as the primary interface.

If the router selects the interface, the interface used to connect the PE router to the site depends on the order in which interfaces are listed in the PE router's configuration. The first operational interface in the set of configured interfaces is chosen to be the designated interface. If this interface fails, the next interface in the list is selected to send and receive traffic for the site.

- Configure multihoming for the site.

The following configuration shows the statements you need to configure to enable VPLS multihoming:

```
[edit routing-instances routing-instance-name]
instance-type vpls;
interface interface-name;
interface interface-name;
protocols vpls {
 site site-name {
 active-interface {
 any;
 primary interface-name;
 }
 interface interface-name;
 interface interface-name;
 multi-homing;
 site-identifier number;
 }
}
route-distinguisher (as-number:id | ip-address:id);
```



**NOTE:** If you add a direct connection between CE devices that are multihomed to the same VPLS site on different PE routers, the traffic can loop and a loss of connectivity might occur. We do not recommend this topology.

Most of these statements are explained in more detail in the rest of this chapter. The following sections explain how to configure the statements that are specific to VPLS multihoming:

- [Specifying an Interface as the Active Interface on page 754](#)
- [Configuring Multihoming on the PE Router on page 755](#)

### Specifying an Interface as the Active Interface

You need to specify one of the interfaces for the multihomed site as the primary interface. If there are multiple interfaces, the remaining interfaces are activated only when the primary interface goes down. If no active interfaces are configured at the site level, all traffic for a VPLS site travels through a single, non-multihomed PE router.

You must configure one of the following options for the **active-interface** statement:

- **any**—One configured interface is randomly designated as the active interface for the VPLS site.
- **primary**—Specify the name of the multihomed interface to be used as the primary interface by the VPLS site.

To specify a multihomed interface as the primary interface for the VPLS site, include the **active-interface** statement:

```
active-interface {
 any;
 primary interface-name;
}
```

You can include this statement at the following hierarchy levels:

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

### Configuring Multihoming on the PE Router

When a CE device is connected to the same VPLS site on more than one PE router, include the **multi-homing** statement on all associated PE routers. Configuration of this statement tracks BGP peers. If no BGP peer is available, VPLS deactivates all active interfaces for a site. To specify that the PE router is part of a multihomed VPLS site, include the **multi-homing** statement:

```
multi-homing;
```

You can include this statement at the following hierarchy levels:

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

Include the **multi-homing** statement on all PE routers associated with a particular VPLS site.

### VPLS Single-Homed Site Configuration

All VPLS single-homed sites are connected to the same default VE device. All interfaces in a VPLS routing instance that are not configured as part of a multihomed site are assumed to be single-homed to the default VE device.

#### Related Documentation

- [VPLS Multihoming Overview on page 705](#)
- [Example: VPLS Multihoming, Improved Convergence Time on page 756](#)
- [active-interface on page 1070](#)
- [multi-homing on page 1157](#)

## Example: VPLS Multihoming, Improved Convergence Time

---

This example shows how to configure a virtual private LAN service (VPLS) employing multihoming to a customer site. This particular VPLS multihoming example shows how to configure a feature that improves the network convergence time in the event a multihomed site needs to switch traffic to its alternate PE router.

- [Requirements on page 756](#)
- [Overview on page 756](#)
- [Configuration on page 757](#)

### Requirements

This example uses the following hardware and software components:

- Three M Series, MX Series, or T Series routers
- Junos OS Release 12.2 or later

If you are using M Series or T Series routers, the PE routers must have either virtual loopback tunnel (**vt**) interfaces or label-switched interfaces (LSIs). On M Series and T Series routers, VPLS uses tunnel-based PICs to create virtual ports on vt interfaces. If you do not have a tunnel-based PIC installed on your M Series or T Series router, you can still configure VPLS by using LSIs to support the virtual ports. Use of LSIs requires Ethernet-based PICs installed in an Enhanced Flexible PIC Concentrator (FPC).

You do not need to use routers for the CE devices. For example, the CE devices can be EX Series Ethernet Switches.

### Overview

All PE routers in a VPLS network operate like a large, distributed Ethernet switch to provide Layer 2 services to attached devices. This example illustrates a network of PE routers and CE devices configured to use VPLS multihoming. The topology consists of six routers: four PE routers and two CE devices. Device CE1 is multihomed to Routers PE1 and PE2. The PE routers are configured with the **best-site** and **mac-flush** statements to improve the convergence time in the event the connection between Device CE1 and one of its multihomed PE routers fails.

This example includes the following settings:

- **best-site**—Uses the B-bit of the control flags bit vector (the third bit counting from the most significant bit) within the Layer 2 information extended community to indicate that the site is preferred. Each VPLS site configured with the **best-site** statement signals to the other PE routers that it is the preferred site. The Layer 2 information extended community includes the following information:
  - Extended community type (2 octets)
  - Encapsulation type (1 octet)
  - Control flags (1 octet)



- Layer 2 MTU (2 octets)
- Reserved (2 octets)

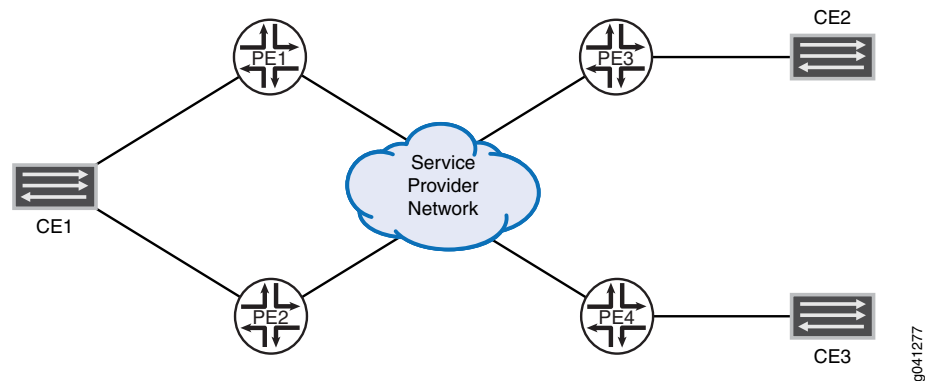
When a neighboring PE router within the VPLS routing instance receives the label block advertisement, it knows that the corresponding PE router is the most preferable router of those remote PE routers multihomed to that site. If a neighboring PE router does not support the best site feature, the standard local site selection process is used. For example, if Router PE1 does not receive a B-bit from any of the label blocks advertisements received from Router PE3, Router PE1 proceeds to assume that Router PE3 does not support the best site feature. It creates a virtual circuit based on its minimum-designated site. For the other PE routers that do support the best site feature, Router PE1 builds virtual circuits using the locally tagged best site.

- **mac-flush**—Enables media access control (MAC) flush processing for the VPLS routing instance or for the mesh group under a VPLS routing instance. MAC flush processing removes MAC addresses from the MAC address database that have been learned dynamically. With the dynamically learned MAC addresses removed, MAC address convergence requires less time to complete.

### Topology

Figure 65 on page 757 shows the topology used in this example. Router PE2 is configured with the **best-site** statement and acts as the preferred gateway for traffic from Device CE1.

Figure 65: VPLS Multihoming Topology with Router PE2 Configured as the Best Site



### 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.

Router PE1:

```
set interfaces fe-0/1/0 encapsulation ethernet-vpls
set interfaces fe-0/1/0 unit 0 family vpls
```

```
set interfaces fe-0/1/2 unit 0 family inet address 10.0.59.14/32
set interfaces fe-0/1/2 unit 0 family iso
set interfaces fe-0/1/2 unit 0 family mpls
set interfaces fe-0/1/3 unit 0 family inet address 10.0.89.14/30
set interfaces fe-0/1/3 unit 0 family iso set interfaces fe-0/1/3 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 192.168.9.1/32
set interfaces lo0 unit 0 family iso address 47.0005.8083.0000.1921.6800.5003.00
set routing-options router-id 192.168.9.1
set protocols mpls interface all
set protocols bgp group int type internal
set protocols bgp group int local-address 192.0.2.1
set protocols bgp group int family l2vpn signaling
set protocols isis level 1 disable
set protocols isis interface fe-0/1/2.0
set protocols isis interface fe-0/1/3.0
set protocols isis interface lo0.0
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0
set routing-instances vpls_1 instance-type vpls
set routing-instances vpls_1 interface fe-0/1/0.0
set routing-instances vpls_1 route-distinguisher 10.255.107.74:1
set routing-instances vpls_1 vrf-target target:65056:1
set routing-instances vpls_1 protocols vpls no-tunnel-services
set routing-instances vpls_1 protocols vpls site site_3 site-identifier 3
set routing-instances vpls_1 protocols vpls site site_3 multi-homing
set routing-instances vpls_1 protocols vpls site site_3 site-preference primary
set routing-instances vpls_1 protocols vpls site site_3 interface fe-0/1/0.0
set routing-instances vpls_1 protocols vpls site site_994 site-identifier 994
set routing-instances vpls_1 protocols vpls mac-flush
```

Router PE2:

```

set interfaces fe-0/1/1 encapsulation ethernet-vpls
set interfaces fe-0/1/1 unit 0 family vpls
set interfaces fe-0/1/2 unit 0 family inet address 10.0.59.13/32
set interfaces fe-0/1/2 unit 0 family iso
set interfaces fe-0/1/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 192.168.5.1/32
set interfaces lo0 unit 0 family iso address 47.0005.8083.0000.1921.6800.5005.00
set routing-options router-id 192.168.5.1
set protocols mpls interface all
set protocols isis level 1 disable
set protocols isis interface fe-0/1/2.0
set protocols isis interface lo0.0
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0
set routing-instances vpls_1 instance-type vpls
set routing-instances vpls_1 interface fe-0/1/1.0
set routing-instances vpls_1 route-distinguisher 10.255.107.76:1
set routing-instances vpls_1 vrf-target target:65056:1
set routing-instances vpls_1 protocols vpls no-tunnel-services
set routing-instances vpls_1 protocols vpls site site_3 site-identifier 3
set routing-instances vpls_1 protocols vpls site site_3 multi-homing
set routing-instances vpls_1 protocols vpls site site_3 site-preference backup
set routing-instances vpls_1 protocols vpls site site_3 interface fe-0/1/1.0
set routing-instances vpls_1 protocols vpls site site_995 site-identifier 995
set routing-instances vpls_1 protocols vpls site site_995 best-site
set routing-instances vpls_1 protocols vpls mac-flush

```

Router PE3:

```

set interfaces fe-1/3/0 unit 0 description "PE3 to PE1"
set interfaces fe-1/3/0 unit 0 family inet address 10.0.89.13/30
set interfaces fe-1/3/0 unit 0 family iso
set interfaces fe-1/3/0 unit 0 family mpls
set interfaces fe-1/3/1 encapsulation ethernet-vpls
set interfaces fe-1/3/1 unit 0 family vpls
set interfaces lo0 unit 0 family inet address 192.168.8.1/32
set interfaces lo0 unit 0 family iso address 47.0005.8083.0000.1921.6800.5002.00
set routing-options router-id 192.168.8.1
set protocols isis level 1 disable
set protocols isis interface fe-1/3/0.0
set protocols isis interface lo0.0
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0
set protocols mpls interface all
set routing-instances vpls_1 instance-type vpls
set routing-instances vpls_1 interface fe-1/3/1.0
set routing-instances vpls_1 route-distinguisher 10.255.107.72:1
set routing-instances vpls_1 vrf-target target:65056:1
set routing-instances vpls_1 protocols vpls no-tunnel-services
set routing-instances vpls_1 protocols vpls site site_2 site-identifier 2
set routing-instances vpls_1 protocols vpls site site_2 interface fe-0/1/0.100
set routing-instances vpls_1 protocols vpls site site_993 site-identifier 993

```

```
set routing-instances vpls_1 protocols vpls mac-flush
```

### Router PE1

#### Step-by-Step Procedure

To configure Router PE1:

1. Configure the interfaces, interface encapsulation, and the protocol families.
 

```
[edit interfaces]
user@PE1# set fe-0/1/0 encapsulation ethernet-vpls
user@PE1# set fe-0/1/0 unit 0 family vpls
user@PE1# set fe-0/1/2 unit 0 family inet address 10.0.59.14/32
user@PE1# set fe-0/1/2 unit 0 family iso
user@PE1# set fe-0/1/2 unit 0 family mpls
user@PE1# set fe-0/1/3 unit 0 family inet address 10.0.89.14/30
user@PE1# set fe-0/1/3 unit 0 family iso set interfaces fe-0/1/3 unit 0 family mpls
user@PE1# set lo0 unit 0 family inet address 192.168.9.1/32
user@PE1# set lo0 unit 0 family iso address
47.0005.8083.0000.1921.6800.5003.00
```
2. Configure the protocol-independent properties.
 

```
[edit routing-options]
user@PE1# set router-id 192.168.9.1
```
3. Configure MPLS on the router's interfaces.
 

```
[edit protocols mpls]
user@PE1# set interface all
```
4. Configure BGP.
 

```
[edit protocols bgp]
user@PE1# set group int type internal
user@PE1# set group int local-address 192.0.2.1
user@PE1# set group int family l2vpn signaling
```
5. Configure IS-IS as the IGP between the PE routers.
 

```
[edit protocols isis]
user@PE1# set level 1 disable
user@PE1# set interface fe-0/1/3.0
user@PE1# set interface lo0.0
```
6. Configure LDP as the signaling protocol for MPLS.
 

```
[edit protocols ldp]
user@PE1# set interface all
user@PE1# set interface fxp0.0 disable
user@PE1# set interface lo0.0
```
7. Configure the VPLS routing instance.
 

Include the **mac-flush** statement to ensure that stale routes are removed from Router PE1 promptly.

```
[edit routing-instances vpls_1]
user@PE1# set instance-type vpls
user@PE1# set interface fe-0/1/0.0
user@PE1# set route-distinguisher 10.255.107.74:1
user@PE1# set vrf-target target:65056:1
```

```

user@PE1# set protocols vpls no-tunnel-services
user@PE1# set protocols vpls site site_3 site-identifier 3
user@PE1# set protocols vpls site site_3 multi-homing
user@PE1# set protocols vpls site site_3 site-preference primary
user@PE1# set protocols vpls site site_3 interface fe-0/1/0.0
user@PE1# set protocols vpls site site_994 site-identifier 994
user@PE1# set protocols vpls mac-flush

```

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

```

user@PE1# show interfaces
fe-0/1/0 {
 encapsulation ethernet-vpls;
 unit 0 {
 family vpls;
 }
}
fe-0/1/2 {
 unit 0 {
 family inet {
 address 10.0.59.14/32;
 }
 family iso;
 family mpls;
 }
}
fe-0/1/3 {
 unit 0 {
 family inet {
 address 10.0.89.14/30;
 }
 family iso;
 family mpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.168.9.1/32;
 }
 family iso {
 address 47.0005.8083.0000.1921.6800.5003.00;
 }
 }
}
}

user@PE1# show protocols
mpls {
 interface all;
}
bgp {
 group int {

```

```

 type internal;
 local-address 192.0.2.1;
 family l2vpn {
 signaling;
 }
 }
}
isis {
 level 1 disable;
 interface fe-0/1/2.0;
 interface fe-0/1/3.0;
 interface lo0.0;
}
ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 interface lo0.0;
}

user@PE1# show routing-instances
vpls_1 {
 instance-type vpls;
 interface fe-0/1/0.0;
 route-distinguisher 10.255.107.74:1;
 vrf-target target:65056:1;
 protocols {
 vpls {
 no-tunnel-services;
 site site_3 {
 site-identifier 3;
 multi-homing;
 site-preference primary;
 interface fe-0/1/0.0;
 }
 site site_994 {
 site-identifier 994;
 }
 mac-flush;
 }
 }
}

user@PE1# show routing-options
router-id 192.168.9.1;

```

## Router PE2

### Step-by-Step Procedure

To configure Router PE2:

1. Configure the interfaces, interface encapsulation, and the protocol families.

```

[edit interfaces]
user@PE2# set fe-0/1/1 encapsulation ethernet-vpls
user@PE2# set fe-0/1/1 unit 0 family vpls
user@PE2# set fe-0/1/2 unit 0 family inet address 10.0.59.13/32

```

```

user@PE2# set fe-0/1/2 unit 0 family iso
user@PE2# set fe-0/1/2 unit 0 family mpls
user@PE2# set lo0 unit 0 family inet address 192.168.5.1/32
user@PE2# set lo0 unit 0 family iso address
47.0005.8083.0000.1921.6800.5005.00

```

2. Configure the protocol-independent properties.

```

[edit routing-options]
user@PE2# set router-id 192.168.5.1

```

3. Configure MPLS on the Router PE2 interfaces.

```

[edit protocols]
user@PE2# set mpls interface all

```

4. Configure the LDP as the signaling protocol for MPLS on the PE router facing interface.

```

[edit protocols ldp]
user@PE2# set interface all
user@PE2# set interface fxp0.0 disable
user@PE2# set interface lo0.0

```

5. Configure IS-IS as the IGP between the PE routers.

```

[edit protocols isis]
user@PE2# set level 1 disable
user@PE2# set interface fe-0/1/2.0
user@PE2# set interface lo0.0

```

6. Configure the VPLS routing instance vpls\_1.

Include the **best-site** statement to ensure that Router PE2 acts as the preferred path for the CE router. Include the **mac-flush** statement to ensure that stale routes are removed from Router PE2 promptly.

```

[edit routing-instances vpls_1]
user@PE2# set instance-type vpls
user@PE2# set interface fe-0/1/1.0
user@PE2# set route-distinguisher 10.255.107.76:1
user@PE2# set vrf-target target:65056:1
user@PE2# set protocols vpls no-tunnel-services
user@PE2# set protocols vpls site site_3 site-identifier 3
user@PE2# set protocols vpls site site_3 multi-homing
user@PE2# set protocols vpls site site_3 site-preference backup
user@PE2# set protocols vpls site site_3 interface fe-0/1/1.0
user@PE2# set protocols vpls site site_995 site-identifier 995
user@PE2# set protocols vpls site site_995 best-site
user@PE2# set protocols vpls mac-flush

```

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

```

user@PE2# show interfaces
fe-0/1/1 {

```

```
encapsulation ethernet-vpls;
unit 0 {
 family vpls;
}
}
fe-0/1/2 {
 unit 0 {
 family inet {
 address 10.0.59.13/32;
 }
 family iso;
 family mpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.168.5.1/32;
 }
 family iso {
 address 47.0005.8083.0000.1921.6800.5005.00;
 }
 }
}
}

user@PE2# show protocols
mpls {
 interface all;
}
isis {
 level 1 disable;
 interface fe-0/1/2.0;
 interface lo0.0;
}
ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 interface lo0.0;
}

user@PE2# show routing-instances
vpls_1 {
 instance-type vpls;
 interface fe-0/1/1.0;
 route-distinguisher 10.255.107.76:1;
 vrf-target target:65056:1;
 protocols {
 vpls {
 no-tunnel-services;
 site site_3 {
 site-identifier 3;
 multi-homing;
 site-preference backup;
 interface fe-0/1/1.0;
 }
 }
 }
}
```



```

 site site_995 {
 site-identifier 995;
 best-site;
 }
 mac-flush;
}
}

user@pe2# show routing-options
router-id 192.168.5.1;

```

### Router PE3

#### Step-by-Step Procedure

To configure Router PE3:

1. Configure the interfaces, interface encapsulation, and the protocol families.

```

[edit interfaces]
user@PE3# set fe-1/3/0 unit 0 description "PE3 to PE1"
user@PE3# set fe-1/3/0 unit 0 family inet address 10.0.89.13/30
user@PE3# set fe-1/3/0 unit 0 family iso
user@PE3# set fe-1/3/0 unit 0 family mpls
user@PE3# set fe-1/3/1 encapsulation ethernet-vpls
user@PE3# set fe-1/3/1 unit 0 family vpls
user@PE3# set lo0 unit 0 family inet address 192.168.8.1/32
user@PE3# set lo0 unit 0 family iso address
47.0005.8083.0000.1921.6800.5002.00

```

2. Configure the protocol-independent properties.

```

[edit routing-options]
user@PE3# set router-id 192.168.8.1

```

3. Configure IS-IS as the IGP between the PE routers.

```

[edit protocols isis]
user@PE3# set level 1 disable
user@PE3# set interface fe-0/1/3.0
user@PE3# set interface lo0.0

```

4. Configure LDP as the signaling protocol for MPLS.

```

[edit protocols ldp]
user@PE3# set interface all
user@PE3# set interface fxp0.0 disable
user@PE3# set interface lo0.0

```

5. Configure the VPLS routing instance.

Include the **mac-flush** statement here to ensure that stale routes are removed from Router PE1 promptly.

```

[edit routing-instances vpls_1]
user@PE3# set instance-type vpls
user@PE3# set interface fe-1/3/1.0
user@PE3# set route-distinguisher 10.255.107.72:1
user@PE3# set vrf-target target:65056:1
user@PE3# set protocols vpls no-tunnel-services
user@PE3# set protocols vpls site site_2 site-identifier 2

```

```
user@PE3# set protocols vpls site site_2 interface fe-0/1/0.100
user@PE3# set protocols vpls site site_993 site-identifier 993
user@PE3# set protocols vpls mac-flush
```

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

```
user@PE3# show interfaces
fe-1/3/0 {
 unit 0 {
 description "PE3 to PE1";
 family inet {
 address 10.0.89.13/30;
 }
 family iso;
 family mpls;
 }
}
fe-1/3/1 {
 encapsulation ethernet-vpls;
 unit 0 {
 family vpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.168.8.1/32;
 }
 family iso {
 address 47.0005.8083.0000.1921.6800.5002.00;
 }
 }
}

user@PE3# show protocols
mpls {
 interface all;
}
bgp {
 group int {
 type internal;
 local-address 192.0.2.2;
 family l2vpn {
 signaling;
 }
 }
}
isis {
 level 1 disable;
 interface fe-1/3/0.0;
 interface lo0.0;
}
```

```

ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 interface lo0.0;
}

user@PE3# show routing-instances
vpls_1 {
 instance-type vpls;
 interface fe-0/1/0.100; ## 'fe-0/1/0.100' is not defined
 route-distinguisher 10.255.107.72:1;
 vrf-target target:65056:1;
 protocols {
 vpls {
 no-tunnel-services;
 site site_2 {
 site-identifier 2;
 interface fe-1/3/1.0;
 }
 site site_993 {
 site-identifier 993;
 }
 mac-flush;
 }
 }
}

user@pe3# show routing-options
router-id 192.168.8.1;

```

- Related Documentation**
- [Configuring VPLS Multihoming \(FEC 128\) on page 753](#)
  - [Example: Configuring VPLS Multihoming \(FEC 129\) on page 769](#)
  - [best-site on page 1076](#)
  - [multi-homing on page 1157](#)

## Example: Configuring VPLS Multihoming (FEC 129)

- [VPLS Multihoming Overview on page 767](#)
- [Example: Configuring VPLS Multihoming \(FEC 129\) on page 769](#)

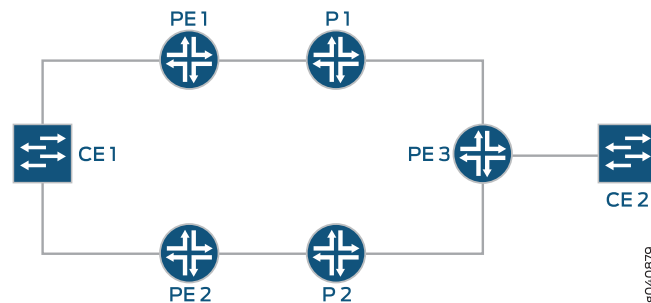
### VPLS Multihoming Overview

Virtual private LAN service (VPLS) multihoming enables you to connect a customer site to two or more PE routers to provide redundant connectivity. A redundant PE router can provide network service to the customer site as soon as a failure is detected. VPLS multihoming helps to maintain VPLS service and traffic forwarding to and from the multihomed site in the event of the following types of network failures:

- PE router to CE device link failure

- PE router failure
- MPLS-reachability failure between the local PE router and a remote PE router

Figure 66: CE Device Multihomed to Two PE Routers



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

Figure 20 on page 247 illustrates how a CE device could be multihomed to two PE routers. Device CE1 is multihomed to Routers PE1 and PE2. Device CE2 has two potential paths to reach Device CE1, but only one path is active at any one time. If Router PE1 were the designated VPLS edge (VE) device (also called a designated forwarder), BGP would signal a pseudowire from Router PE3 to Router PE1. If a failure occurred over this path, Router PE2 would be made the designated VE device, and BGP would re-signal the pseudowire from Router PE3 to Router PE2.

Multihomed PE routers advertise network layer reachability information (NLRI) for the multihomed site to the other PE routers in the VPLS network. The NLRI includes the site ID for the multihomed PE routers. For all of the PE routers multihomed to the same CE device, you need to configure the same site ID. The remote VPLS PE routers use the site ID to determine where to forward traffic addressed to the customer site. To avoid route collisions, the site ID shared by the multihomed PE routers must be different than the site IDs configured on the remote PE routers in the VPLS network.

Although you configure the same site ID for each of the PE routers multihomed to the same CE device, you can configure unique values for other parameters, such as the route distinguisher. These values help to determine which multihomed PE router is selected as the designated VE device to be used to reach the customer site.



**BEST PRACTICE:** We recommend that you configure unique route distinguishers for each multihomed PE router. Configuring unique route distinguishers helps with faster convergence when the connection to a primary multihomed PE router goes down. If you configure unique route distinguishers, the other PE routers in the VPLS network must maintain additional state for the multihomed PE routers.

Remote PE routers in the VPLS network need to determine which of the multihomed PE routers should forward traffic to reach the CE device. To make this determination, remote PE routers use the VPLS path-selection process to select one of the multihomed PE routers based on its NLRI advertisement. Because remote PE routers pick only one of the NLRI advertisements, it establishes a pseudowire to only one of the multihomed PE routers, the PE router that originated the winning advertisement. This prevents multiple paths from being created between sites in the network, preventing the formation of Layer 2 loops. If the selected PE router fails, all PE routers in the network automatically switch to the backup PE router and establish new pseudowires to it.



**BEST PRACTICE:** To prevent the formation of Layer 2 loops between the CE devices and the multihomed PE routers, we recommend that you employ the Spanning Tree Protocol (STP) on your CE devices. Layer 2 loops can form due to incorrect configuration. Temporary Layer 2 loops can also form during convergence after a change in the network topology.

The PE routers run the BGP path selection procedure on locally originated and received Layer 2 route advertisements to establish that the routes are suitable for advertisement to other peers, such as BGP route reflectors. If a PE router in a VPLS network is also a route reflector, the path selection process for the multihomed site has no effect on the path selection process performed by this PE router for the purpose of reflecting Layer 2 routes. Layer 2 prefixes that have different route distinguishers are considered to have different NLRIs for route reflection. The VPLS path selection process enables the route reflector to reflect all routes that have different route distinguishers to the route reflector clients, even though only one of these routes is used to create the VPLS pseudowire to the multihomed site.

Junos OS supports VPLS multihoming for both FEC 128 and FEC 129. Support for FEC 129 is added in Junos OS Release 12.3.

### Example: Configuring VPLS Multihoming (FEC 129)

This example shows how to configure virtual private LAN service (VPLS) multihoming. Multihoming allows a customer site to connect to multiple provider edge (PE) routers. A VPLS site multihomed to two or more PE routers provides redundant connectivity in the event of a PE router-to-CE device link failure or the failure of a PE router. The example demonstrates BGP-based multihoming support for FEC 129 VPLS (also known as LDP VPLS with BGP-based autodiscovery).

- [Requirements on page 769](#)
- [Overview on page 770](#)
- [Configuration on page 771](#)
- [Verification on page 778](#)

#### Requirements

This example has the following hardware and software requirements:

- One or more CE devices to represent a VPLS site.

- Two or more PE devices.
- Junos OS Release 12.3 or later running on the PE devices that are connected to the multihomed VPLS site.

## Overview

---

BGP-based VPLS autodiscovery (FEC 129) enables each VPLS PE router to discover the other PE routers that are in the same VPLS domain. VPLS autodiscovery also automatically detects when PE routers are added or removed from the VPLS domain. You do not need to manually configure the VPLS and maintain the configuration when a PE router is added or deleted. VPLS autodiscovery uses BGP to discover the VPLS members and to set up and tear down pseudowires in the VPLS.

BGP multihoming enables you to connect a customer site to two or more PE routers to provide redundant connectivity while preventing the formation of Layer 2 loops in the service provider's network. The redundant connectivity maintains the VPLS service and traffic forwarding to and from the multihomed site in the event of a PE router-to-CE device link failure, the failure of a PE router, or an MPLS reachability failure between the local PE router and a remote PE router. A redundant PE router can begin providing service to the customer site as soon as the failure is detected.

When a CE device connects to multiple PE routers, each of these routers advertises reachability for the multihomed site—routes that have the same site ID in the Layer 2 network layer reachability information (NLRI). The other PE routers in the network use a BGP path selection process to select only one of the advertising routers to which they send traffic destined for the CE device. This path selection process eliminates Layer 2 loops in the VPLS network.

Autodiscovery is not specifically related to multihoming. Autodiscovery is not required for multihoming to work. They are two separate features. That said, the meaning of FEC 129 is that VPLS does autodiscovery. So when you configure multihoming for FEC 129, you must also, by definition, configure autodiscovery (with the **auto-discovery-only** statement).

There are two places in the configuration where you can configure VPLS multihoming. One is for FEC 128, and the other is for FEC 129:

- For FEC 128—**routing-instances *instance-name* protocols vpls site *site-name* multi-homing**
- For FEC 129—**routing-instances *instance-name* protocols vpls multi-homing**

The following statements are used for configuring multihoming for FEC 129:

```
[edit routing-instances instance-name protocols vpls]
multi-homing {
 peer-active;
 site site-name {
 active-interface interface-name {
 any;
 primary interface-name;
 }
 identifier identifier;
```

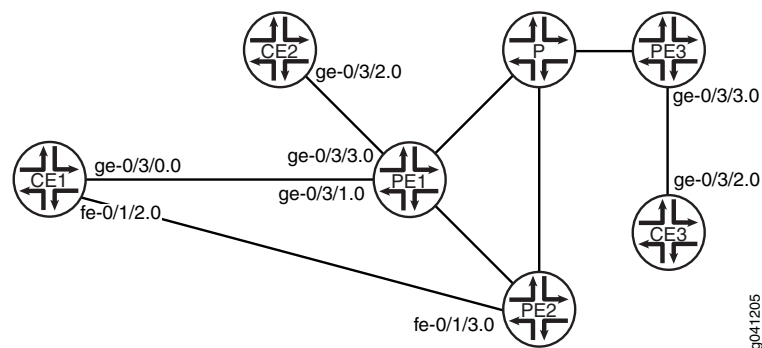
```

interface interface-name {
 preference preference-value;
}
peer-active;
preference (preference-value | backup | primary);
}
}

```

This example shows Device CE1 multihomed to Router PE1 and Router PE2. In addition, Device CE2 is single-homed to Router PE1. Device PE3 is the remote PE router, connected to Device CE3. Multihoming is not enabled on Device PE3. “CLI Quick Configuration” on page 771 shows the configuration for all of the devices in Figure 67 on page 771. The section “Configuring Device PE1” on page 774 has step-by-step instructions for configuring Device PE1.

Figure 67: Topology for FEC 129 Multihoming



### 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 PE1**

```

set interfaces ge-0/3/3 encapsulation ethernet-vpls
set interfaces ge-0/3/3 unit 0 description PE1-to-CE2
set interfaces ge-0/3/3 unit 0 family vpls
set interfaces ge-0/3/1 encapsulation ethernet-vpls
set interfaces ge-0/3/1 unit 0 description PE1-to-CE1
set interfaces ge-0/3/1 unit 0 family vpls
set interfaces ge-1/2/0 unit 1 description PE1-to-P
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 ge-1/2/1 unit 5 description PE1-to-PE2
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 lo0 unit 2 family inet address 192.0.2.2/24
set protocols mpls interface ge-1/2/0.1
set protocols mpls interface ge-1/2/1.5
set protocols bgp local-address 192.0.2.2
set protocols bgp group pe-pe type internal
set protocols bgp group pe-pe family l2vpn auto-discovery-only
set protocols bgp group pe-pe family l2vpn signaling

```

```

set protocols bgp group pe-pe neighbor 192.0.2.3
set protocols bgp group pe-pe neighbor 192.0.2.4
set protocols bgp group pe-pe neighbor 192.0.2.5
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface ge-1/2/0.1
set protocols ospf area 0.0.0.0 interface ge-1/2/1.5
set protocols ospf area 0.0.0.0 interface lo0.2 passive
set protocols ldp interface ge-1/2/0.1
set protocols ldp interface ge-1/2/1.5
set protocols ldp interface lo0.2
set routing-instances green instance-type vpls
set routing-instances green interface ge-0/3/1.0
set routing-instances green interface ge-0/3/3.0
set routing-instances green route-distinguisher 192.0.2.2:1
set routing-instances green l2vpn-id l2vpn-id:100:100
set routing-instances green vrf-target target:100:100
set routing-instances green protocols vpls no-tunnel-services
set routing-instances green protocols vpls oam ping-interval 600
set routing-instances green protocols vpls oam bfd-liveness-detection minimum-interval
 200
set routing-instances green protocols vpls multi-homing site test identifier 1
set routing-instances green protocols vpls multi-homing site test interface ge-0/3/1.0
set routing-options router-id 192.0.2.2
set routing-options autonomous-system 100

```

```

Device PE2
set interfaces fe-0/1/3 encapsulation ethernet-vpls
set interfaces fe-0/1/3 unit 0 description PE2-to-CE1
set interfaces fe-0/1/3 unit 0 family vpls
set interfaces ge-1/2/0 unit 6 description PE2-to-PE1
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-1/2/2 unit 10 description PE2-to-P
set interfaces ge-1/2/2 unit 10 family inet address 10.1.1.10/30
set interfaces ge-1/2/2 unit 10 family mpls
set interfaces lo0 unit 4 family inet address 192.0.2.4/24
set protocols mpls interface ge-1/2/0.6
set protocols mpls interface ge-1/2/2.10
set protocols bgp local-address 192.0.2.4
set protocols bgp group pe-pe type internal
set protocols bgp group pe-pe family l2vpn auto-discovery-only
set protocols bgp group pe-pe family l2vpn signaling
set protocols bgp group pe-pe neighbor 192.0.2.2
set protocols bgp group pe-pe neighbor 192.0.2.3
set protocols bgp group pe-pe neighbor 192.0.2.5
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface ge-1/2/0.6
set protocols ospf area 0.0.0.0 interface ge-1/2/2.10
set protocols ospf area 0.0.0.0 interface lo0.4 passive
set protocols ldp interface ge-1/2/0.6
set protocols ldp interface ge-1/2/2.10
set protocols ldp interface lo0.4
set routing-instances green instance-type vpls
set routing-instances green interface fe-0/1/3.0
set routing-instances green route-distinguisher 192.0.2.4:1
set routing-instances green l2vpn-id l2vpn-id:100:100
set routing-instances green vrf-target target:100:100

```



```

set routing-instances green protocols vpls no-tunnel-services
set routing-instances green protocols vpls oam ping-interval 600
set routing-instances green protocols vpls oam bfd-liveness-detection minimum-interval
 200
set routing-instances green protocols vpls multi-homing site test identifier 1
set routing-instances green protocols vpls multi-homing site test interface fe-0/1/3.0
set routing-options router-id 192.0.2.4
set routing-options autonomous-system 100

```

|            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device PE3 | <pre> set interfaces ge-0/3/3 unit 0 set interfaces ge-1/2/0 unit 14 description PE3-to-P 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 lo0 unit 5 family inet address 192.0.2.5/32 set protocols rsvp interface ge-1/2/0.14 set protocols mpls interface ge-1/2/0.14 set protocols bgp local-address 192.0.2.5 set protocols bgp group pe-pe type internal set protocols bgp group pe-pe family l2vpn auto-discovery-only set protocols bgp group pe-pe family l2vpn signaling set protocols bgp group pe-pe neighbor 192.0.2.2 set protocols bgp group pe-pe neighbor 192.0.2.3 set protocols bgp group pe-pe neighbor 192.0.2.4 set protocols ospf traffic-engineering set protocols ospf area 0.0.0.0 interface ge-1/2/0.14 set protocols ospf area 0.0.0.0 interface lo0.5 passive set protocols ldp interface ge-1/2/0.14 set protocols ldp interface lo0.5 set routing-instances green instance-type vpls set routing-instances green interface ge-0/3/3.0 set routing-instances green route-distinguisher 192.0.2.5:100 set routing-instances green l2vpn-id l2vpn-id:100:100 set routing-instances green vrf-target target:100:100 set routing-instances green protocols vpls no-tunnel-services set routing-instances green protocols vpls oam ping-interval 600 set routing-instances green protocols vpls oam bfd-liveness-detection minimum-interval   200 set routing-instances green protocols vpls oam ping-interval 600 set routing-instances green protocols vpls oam bfd-liveness-detection minimum-interval   200 set routing-options router-id 192.0.2.5 set routing-options autonomous-system 100 </pre> |
| Device CE1 | <pre> set interfaces ge-0/3/0 unit 0 description CE1-to-PE1 set interfaces ge-0/3/0 unit 0 family inet address 203.0.113.5/24 set interfaces fe-0/1/2 unit 0 description CE1-to-PE2 set interfaces fe-0/1/2 unit 0 family inet address 203.0.113.1/24 </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Device CE2 | <pre> set interfaces ge-0/3/2 unit 0 description CE2-to-PE1 set interfaces ge-0/3/2 unit 0 family inet address 203.0.113.6/24 </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Device CE3 | <pre> set interfaces ge-0/3/2 unit 0 description CE3-to-PE3 set interfaces ge-0/3/2 unit 0 family inet address 203.0.113.7/24 </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Device P   | <pre> set interfaces ge-1/2/0 unit 2 description P-to-PE1 </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

```

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-3/2/0 unit 9 description P-to-PE2
set interfaces ge-3/2/0 unit 9 family inet address 10.1.1.9/30
set interfaces ge-3/2/0 unit 9 family mpls
set interfaces ge-4/2/0 unit 13 description P-to-PE3
set interfaces ge-4/2/0 unit 13 encapsulation ethernet
set interfaces ge-4/2/0 unit 13 peer-unit 14
set interfaces ge-4/2/0 unit 13 family inet address 10.1.1.13/30
set interfaces ge-4/2/0 unit 13 family mpls
set interfaces lo0 unit 3 family inet address 192.0.2.3/24
set protocols mpls interface ge-1/2/0.2
set protocols mpls interface ge-3/2/0.9
set protocols mpls interface ge-4/2/0.13
set protocols bgp local-address 192.0.2.3
set protocols bgp group pe-pe type internal
set protocols bgp group pe-pe family l2vpn signaling
set protocols bgp group pe-pe neighbor 192.0.2.2
set protocols bgp group pe-pe neighbor 192.0.2.4
set protocols bgp group pe-pe neighbor 192.0.2.5
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface ge-1/2/0.2
set protocols ospf area 0.0.0.0 interface ge-3/2/0.9
set protocols ospf area 0.0.0.0 interface ge-4/2/0.13
set protocols ospf area 0.0.0.0 interface lo0.3 passive
set protocols ldp interface ge-1/2/0.2
set protocols ldp interface ge-3/2/0.9
set protocols ldp interface ge-4/2/0.13
set protocols ldp interface lo0.3
set routing-options router-id 192.0.2.3
set routing-options autonomous-system 100

```

### Configuring Device PE1

**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 Device PE1:

1. Configure the interfaces.

Configure **family mpls** on the provider-facing interfaces. Configure **family vpls** on the customer-facing interfaces.

```
[edit interfaces]
```

```

user@PE1# set ge-0/3/3 encapsulation ethernet-vpls
user@PE1# set ge-0/3/3 unit 0 description PE1-to-CE2
user@PE1# set ge-0/3/3 unit 0 family vpls

```

```

user@PE1# set ge-0/3/1 encapsulation ethernet-vpls
user@PE1# set ge-0/3/1 unit 0 description PE1-to-CE1
user@PE1# set ge-0/3/1 unit 0 family vpls

```

```
user@PE1# set ge-1/2/0 unit 1 description PE1-to-P
```

```
user@PE1# set ge-1/2/0 unit 1 family inet address 10.1.1.1/30
user@PE1# set ge-1/2/0 unit 1 family mpls
```

```
user@PE1# set ge-1/2/1 unit 5 description PE1-to-PE2
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 lo0 unit 2 family inet address 192.0.2.2/24
```

2. Configure the interior gateway protocol (IGP) and signaling protocols on the provider-facing interfaces.

The **traffic-engineering** statement enables OSPF to advertise the label-switched path (LSP) metric in summary link-state advertisements (LSAs).

```
[edit protocols]
user@PE1# set ldp interface ge-1/2/0.1
user@PE1# set ldp interface ge-1/2/1.5
user@PE1# set ldp interface lo0.2

user@PE1# set mpls interface ge-1/2/0.1
user@PE1# set mpls interface ge-1/2/1.5

user@PE1# set ospf traffic-engineering
user@PE1# set ospf area 0.0.0.0 interface ge-1/2/0.1
user@PE1# set ospf area 0.0.0.0 interface ge-1/2/1.5
user@PE1# set ospf area 0.0.0.0 interface lo0.2 passive
```

3. Configure BGP.

The **auto-discovery-only** statement notifies the routing process (rpd) to expect autodiscovery-related NLRI messages so that information can be deciphered and used by LDP and VPLS. The **auto-discovery-only** statement must be configured on all PE routers in a VPLS. If you configure route reflection, the **auto-discovery-only** statement is also required on provider (P) routers that act as the route reflector in supporting FEC 129-related updates.

For interoperation scenarios in which a PE router must support both types of NLRI (FEC 128 and FEC 129), this example also includes the **signaling** statement.

```
[edit protocols bgp]
user@PE1# set local-address 192.0.2.2
user@PE1# set group pe-pe type internal
user@PE1# set group pe-pe family l2vpn auto-discovery-only
user@PE1# set group pe-pe family l2vpn signaling
user@PE1# set group pe-pe neighbor 192.0.2.3
user@PE1# set group pe-pe neighbor 192.0.2.4
user@PE1# set group pe-pe neighbor 192.0.2.5
```

4. Configure the routing instance.

Both CE-facing interfaces are included in the routing instance. Only the multihomed interface is included in the multihoming site.

As a convention, the route distinguisher is composed of Device PE1's loopback interface address and the multihoming site identifier.

```
[edit routing-instances green]
user@PE1# set instance-type vpls
user@PE1# set interface ge-0/3/1.0
user@PE1# set interface ge-0/3/3.0
user@PE1# set route-distinguisher 192.0.2.2:1
user@PE1# set l2vpn-id l2vpn-id:100:100
user@PE1# set vrf-target target:100:100
user@PE1# set protocols vpls no-tunnel-services
user@PE1# set protocols vpls multi-homing site test identifier 1
user@PE1# set protocols vpls multi-homing site test interface ge-0/3/1.0
```

5. (Optional) Configure bidirectional forwarding detection (BFD) for FEC 129 VPLS.

```
[edit routing-instances green]
user@PE1# set protocols vpls oam ping-interval 600
user@PE1# set protocols vpls oam bfd-liveness-detection minimum-interval 200
```

6. Configure the autonomous system (AS) number and router ID.

```
[edit routing-options]
user@PE1# set router-id 192.0.2.2
user@PE1# set autonomous-system 100
```

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

```
user@PE1# show interfaces
ge-0/3/1 {
 encapsulation ethernet-vpls;
 unit 0 {
 description PE1-to-CE1;
 family vpls;
 }
}
ge-0/3/3 {
 encapsulation ethernet-vpls;
 unit 0 {
 description PE1-to-CE2;
 family vpls;
 }
}
ge-1/2/0 {
 unit 1 {
 description PE1-to-P;
 family inet {
 address 10.1.1.1/30;
 }
 family mpls;
 }
}
ge-1/2/1 {
 unit 5 {
 description PE1-to-PE2;
 family inet {
```

```

 address 10.1.1.5/30;
 }
 family mpls;
}
}
lo0 {
 unit 2 {
 family inet {
 address 192.0.2.2/24;
 }
 }
}

user@PE1# show protocols
mpls {
 interface ge-1/2/0.1;
 interface ge-1/2/1.5;
}
bgp {
 local-address 192.0.2.2;
 group pe-pe {
 type internal;
 family l2vpn {
 auto-discovery-only;
 signaling;
 }
 neighbor 192.0.2.3;
 neighbor 192.0.2.4;
 neighbor 192.0.2.5;
 }
}
ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface ge-1/2/0.1;
 interface ge-1/2/1.5;
 interface lo0.2 {
 passive;
 }
 }
}
ldp {
 interface ge-1/2/0.1;
 interface ge-1/2/1.5;
 interface lo0.2;
}

user@PE1# show routing-instances
green {
 instance-type vpls;
 interface ge-0/3/1.0;
 interface ge-0/3/3.0;
 route-distinguisher 192.0.2.2:100;
 l2vpn-id l2vpn-id:100:100;
 vrf-target target:100:100;
 protocols {
 vpls {

```

```

no-tunnel-services;
oam {
 ping-interval 600;
 bfd-liveness-detection {
 minimum-interval 200;
 }
}
multi-homing {
 site test {
 identifier 1;
 interface ge-0/3/1.0;
 }
}
}
}

```

```

user@PE1# show routing-options
router-id 192.0.2.2;
autonomous-system 100;

```

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

## Verification

Confirm that the configuration is working properly.

- [Verifying That Multihoming Is Operational on page 778](#)
- [Checking the Multihoming Routes on page 779](#)
- [Checking the BFD Sessions on page 780](#)
- [Pinging the Remote PE Router in the VPLS Domain on page 780](#)

### Verifying That Multihoming Is Operational

**Purpose** Verify that multihoming is operational.

**Action** From operational mode, enter the **show vpls connections extensive** command.

```

user@PE1> show vpls connections extensive
Layer-2 VPN connections:

```

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -> -- only outbound connection is up           |
| CN -- circuit not provisioned    | <- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unknown connection status  | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not available              |
| BK -- Backup connection          | ST -- Standby connection                       |
| PF -- Profile parse failure      | PB -- Profile busy                             |

```

RS -- remote site standby SN -- Static Neighbor
LB -- Local site not best-site RB -- Remote site not best-site
VM -- VLAN ID mismatch

Legend for interface status
Up -- operational
Dn -- down

Instance: green
 L2vpn-id: 100:100
 Local-id: 192.0.2.2
 Number of local interfaces: 2
 Number of local interfaces up: 2
 ge-0/3/1.0
 ge-0/3/3.0
 lsi.101711873
192.0.2.4 neighbor 192.0.2.4 Intf - vpls green local-id 192.0.2.2 remote-id
 Remote-id Type St Time last up # Up trans
 192.0.2.4 rmt Up Jan 31 13:49:52 2012 1
 Remote PE: 192.0.2.4, Negotiated control-word: No
 Incoming label: 262146, Outgoing label: 262146
 Local interface: lsi.101711873, Status: Up, Encapsulation: ETHERNET
 Description: Intf - vpls green local-id 192.0.2.2 remote-id 192.0.2.4
neighbor 192.0.2.4
 Connection History:
 Jan 31 13:49:52 2012 status update timer
 Jan 31 13:49:52 2012 PE route changed
 Jan 31 13:49:52 2012 Out lbl Update 262146
 Jan 31 13:49:52 2012 In lbl Update 262146
 Jan 31 13:49:52 2012 loc intf up lsi.101711873
Multi-home:
 Local-site Id Pref State
 test 1 100 Up
 Number of interfaces: 1
 Number of interfaces up: 1
 ge-0/3/1.0
 Received multi-homing advertisements:
 Remote-PE Pref flag Description
 192.0.2.4 100 0x0

```

**Meaning** The output shows the status of multihoming for routing instance green.

### Checking the Multihoming Routes

**Purpose** Verify that the expected routes are identified as multihoming.

**Action** From operational mode, enter the **show route table bgp.l2vpn.0** and **show route table green.l2vpn.0** commands.

```

user@PE1> show route table bgp.l2vpn.0
bgp.l2vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.4:100:192.0.2.4/96 AD
 *[BGP/170] 1d 03:10:45, localpref 100, from 192.0.2.4
 AS path: I, validation-state: unverified
 > via ge-1/2/1.5
192.0.2.4:100:1:0/96 MH
 *[BGP/170] 1d 03:10:45, localpref 100, from 192.0.2.4

```

```

AS path: I, validation-state: unverified
> via ge-1/2/1.5

user@PE1> show route table green.l2vpn.0
green.l2vpn.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.2:100:192.0.2.2/96 AD
 *[VPLS/170] 1d 03:11:03, metric2 1
 Indirect
192.0.2.4:100:192.0.2.4/96 AD
 *[BGP/170] 1d 03:11:02, localpref 100, from 192.0.2.4
 AS path: I, validation-state: unverified
 > via ge-1/2/1.5
192.0.2.2:100:1:0/96 MH
 *[VPLS/170] 1d 03:11:03, metric2 1
 Indirect
192.0.2.4:100:1:0/96 MH
 *[BGP/170] 1d 03:11:02, localpref 100, from 192.0.2.4
 AS path: I, validation-state: unverified
 > via ge-1/2/1.5
192.0.2.4:NoCtrlWord:5:100:100:192.0.2.2:192.0.2.4/176
 *[VPLS/7] 1d 03:11:02, metric2 1
 > via ge-1/2/1.5
192.0.2.4:NoCtrlWord:5:100:100:192.0.2.4:192.0.2.2/176
 *[LDP/9] 1d 03:11:02
 Discard

```

**Meaning** MH in the output indicates a multihoming route. AD indicates autodiscovery.

### Checking the BFD Sessions

**Purpose** Verify that the BFD session status is operational.

**Action** From operational mode, enter the **show bfd session** command.

```

user@PE1> show bfd session

Address State Interface Detect Transmit
172.16.0.1 Up ge-1/2/1.5 0.600 0.200 3
172.16.0.1 Up ge-1/2/0.1 0.600 0.200 3

2 sessions, 2 clients
Cumulative transmit rate 10.0 pps, cumulative receive rate 10.0 pps

```

**Meaning** Up in the **State** field indicates that BFD is working.

### Pinging the Remote PE Router in the VPLS Domain

**Purpose** Check the operability of the MPLS Layer 2 virtual private network (VPN) connection.

**Action** From operational mode, enter the **ping mpls l2vpn** command with the **fec129** option.

```

user@PE1> ping mpls l2vpn fec129 instance green remote-id 192.0.2.5 remote-pe-address 192.0.2.5
!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss

```



**Meaning** The output shows that the ping operation is successful, meaning that the LSP for a FEC 129 Layer 2 VPN connection is reachable.

**Related Documentation**

- [Example: Configuring BGP Autodiscovery for LDP VPLS on page 725](#)
- [Example: Configuring BGP Autodiscovery for LDP VPLS with User-Defined Mesh Groups on page 742](#)

## Next-Generation VPLS for Multicast with Multihoming Overview

VPLS emulates the broadcast domain of a LAN across an MPLS network cloud. Traditional MPLS implementations of VPLS require that all participating ingress PE routers make separate copies of each broadcast or multicast packet to send to all other PE routers that are part of the VPLS site for the same extended LAN. In a large virtual private network (VPN), replication overhead can be significant for each ingress router and its attached core-facing links.

Junos OS offers the following VPLS enhancements which provide redundancy for VPLS between PE and CE routers:

- Redundancy using BGP for multihomed links between PE and CE devices— Juniper Networks integrates the local preference and path selection capability of BGP with VPLS to allow a CE Ethernet switch to have a backup path across the network.
- Redundancy using the Spanning Tree Protocol (STP) for multihomed links between PE and CE devices— Various versions of STP can be used in the CE network to avoid loops in a multihoming environment. The provider does not have any control over this customer network configuration. The provider can also implement BGP-based loop avoidance as an additional measure to avoid loops.

The following standardized VPLS implementations are supported by the Internet Engineering Task Force (IETF):

- RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*
- RFC 4762, *Virtual Private LAN Service (VPLS) Using LDP Signaling*

For more information about the basic configuration of next-generation VPLS, see the Technology Overview *Next-Generation VPLS Using Point-to-Multipoint LSPs for Unicast and Multicast Forwarding*.

For a detailed technology overview of VPLS, you can refer to *LDP-BGP VPLS Interworking* at the following location:

<http://www.juniper.net/us/en/local/pdf/whitepapers/2000282-en.pdf> .

### Redundancy Using BGP for Multihomed Links between PE and CE Routers

Juniper Networks implements a BGP-based multihoming solution to provide redundancy for VPLS between PE and CE routers.

In this implementation:

- VPLS-enabled PE routers (also called VPLS PE routers) collectively elect one of the VPLS PE routers, to which a site is multihomed, as the designated forwarder of traffic between this site and all other sites.
- All the other VPLS PE routers, to which the same site is connected, do not forward traffic to or from the site.
- Essentially all VPLS PE routers behave as if the site is singlehomed to the VPLS PE router that is the designated forwarder.
- Service providers are able to prevent well-known Layer 2 loops without relying on the customer's STP configuration.
- Customers can still run STP as a fallback strategy to prevent loops that are formed without the service provider's knowledge.

The benefits of multihoming include:

- Redundancy of the link connecting the PE router and the CE device.
- Redundancy of the directly connected PE routers.
- Faster convergence when there is a link failure between a PE router and CE device.
- The same BGP attributes are used to configure primary and backup links.

## Operation of Next-Generation VPLS for Multicast with Multihoming Using BGP

VPLS provides a multipoint-to-multipoint Ethernet service that can span one or more metro areas and multiple sites. VPLS provides connectivity as if these sites are attached to the same Ethernet LAN.

VPLS uses an IP and MPLS service provider infrastructure. From the service provider's point of view, using IP and MPLS routing protocols and procedures instead of STP, and using MPLS labels instead of VLAN identifiers (IDs), significantly improves the scalability of the VPLS service.

### Single CE Site Connected to Multiple VPLS PE Routers

This section describes the process used to elect a single designated forwarder for a multihomed site.

For a multihomed site, all the PE routers in the VPLS instance elect the same designated forwarder PE router using the BGP VPLS multihoming procedure. Only elected designated forwarders forward traffic to and receive traffic from the multihomed site. All other PE routers where this multihomed site is present do not participate in forwarding for that site.

All remote PE routers are aware of the designated forwarder PE router for each multihomed site and do not create a pseudowire to the PE routers that are not the designated forwarder for the multihomed site.

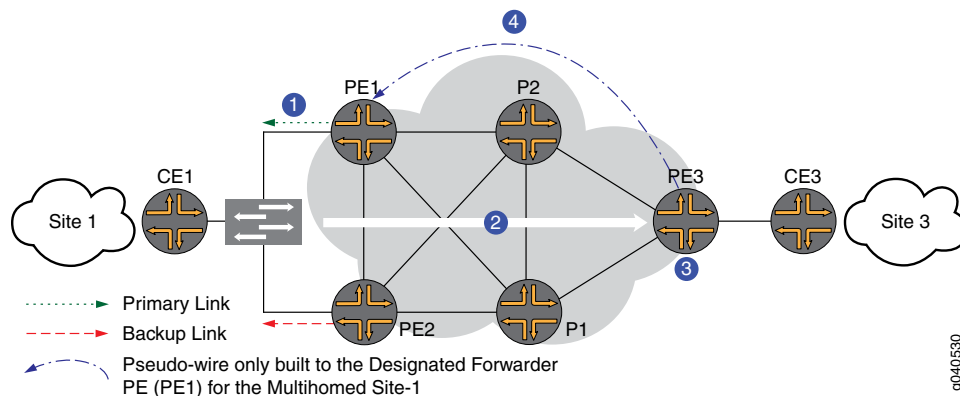
In [Figure 68 on page 784](#):

- The same site ID (sometimes known as a VPLS edge identifier or VE ID) is configured on all VPLS PE routers to which a site is multihomed.
- All PE routers are aware of which sites are multihomed since they see multiple advertisements with the same site ID.
- One of the VPLS PE routers is selected as the designated forwarder for this site by all PE routers based on a deterministic algorithm.
- The algorithm selects the VPLS PE router that originates the best advertisement with a particular site ID as the designated forwarder. There are two possible selection methods:
  - BGP path selection on the route reflector and the PE routers
  - VPLS site selection on the PE router only
- If multiple network layer reachability information (NLRI) advertisements have the same route distinguisher and site ID, the router uses BGP path selection rules to select the best path. The BGP rules are:
  - Always prefer advertisements that do not have the down bit set over ones that do have this bit set.
  - Prefer the advertisement with the higher local preference.
  - Use the configurable per-site site preference to set the BGP local preference in the advertisement and influence the choice of the designated forwarder.
  - Ignore the interior gateway protocol (IGP) metric while doing path selection because the choice of designated forwarder must be the same on all PE routers.
- Among advertisements with the same route distinguisher, apply VPLS site selection rules (a subset of BGP path selection rules) to pick the select advertisement.

[Figure 68 on page 784](#) illustrates the following four-step process to select the designated forwarder and create the pseudowire:

1. Router PE1 and Router PE2 both have the same site ID (Site 1) for Router CE1.  
Router PE1 has a better local preference of 65535 and is configured as the primary router.
2. Router PE3 receives the BGP NLRI advertisement from Router PE1 and Router PE2 with the local preferences of 65535 and 1, respectively.
3. Router PE3 runs the BGP path selection algorithm and selects Router PE1 as the designated forwarder VPLS edge PE router for Site 1.
4. Router PE3 creates the pseudowire only to Router PE1, which helps to save bandwidth in the network core.

Figure 68: Single CE Site Multihomed with Two PE Routers



9040530

The resulting VPLS PE router roles for Site 1 are:

- Router PE1 is the designated forwarder VPLS edge PE router.
- Router PE2 is the non-designated forwarder VPLS edge PE router.
- Router PE3 is the remote VPLS edge PE router.

All the interfaces linking the CE and PE devices that are connected to the designated forwarder VPLS PE router, are marked **Up** and **forwarding** in **show** command output.

All the interfaces linking the CE and PE devices on the non-designated forwarder VPLS PE router, are marked **vc-down** in **show** command output. The router does not send traffic or forward received traffic on these interfaces.

Remote VPLS PE routers establish pseudowires only to the designated PE router, and tear down any pseudowires to the non-designated PE router.

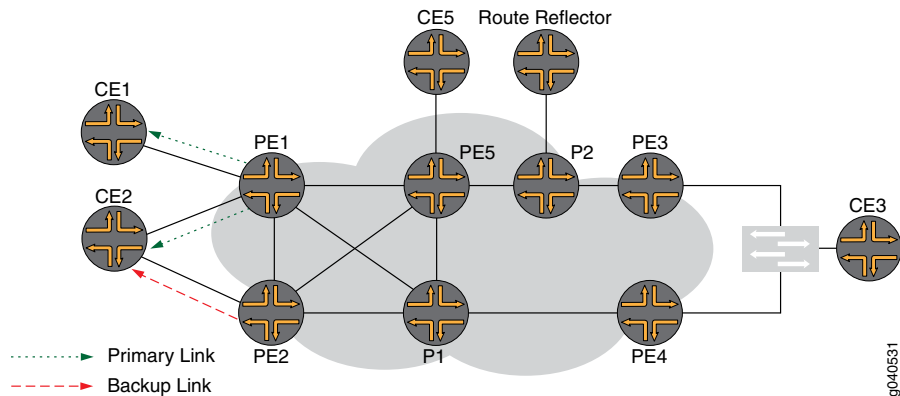
### Multiple CE Sites Connected to a Single VPLS PE Router for Link Redundancy

This section describe some of the operational details of multiple CE sites connected to a single VPLS PE router.

In [Figure 69 on page 785](#):

- Router CE2 is multihomed to Router PE1 and Router PE2.
- Router CE1 is singlehomed to Router PE1.

Figure 69: Two CE Sites Multihomed to a Single PE Router on Different Line Cards



The scenario shown in Figure 2 is common. Your network might have a single PE router in a remote area, but you would like to multihome a Layer 2 network to different Flexible PIC Concentrators (FPCs) on the same PE router. This configuration provides link redundancy on the CE devices and link redundancy on the links between the CE and PE devices, but limited link redundancy on PE devices. In this case, you need the ability to configure a site to use a single active interface for forwarding.

In this scenario:

- Path selection is done per site to determine if a PE router is the designated forwarder for that site or not.
- Only a single pseudowire is established between any two PE routers, even if one or both of them have multiple designated PE routers.



**NOTE:** A pseudowire between two PE routers is always established between the designated sites with the minimum site IDs on the two PE routers.

- Establishing a single pseudowire avoids the need to maintain multiple flooding and media access control (MAC) address tables per instance (one per site) on each PE router.
- The local interfaces are marked **vc-down** in the **show** command output where a site is connected to the non-designated forwarder router.
- When a designated site on a PE router fails, all MAC addresses from this remote PE router have to be learned again, since the router does not know the exact site where the MAC addresses were originally learned from.

## Implementation of Redundancy Using VPLS Multihomed Links Between PE and CE Devices

You might need to multihome a CE device to multiple PE routers without causing a Layer 2 forwarding loop. This is not a problem if the CE device is a router, since no Layer 2 loops

can form when using a router. However, if the CE device is a Layer 2 device, like a hub or switch, multihoming it to two PE routers can cause a Layer 2 loop.

You can use one of the following methods to prevent the Layer 2 loop:

- BGP-based primary and backup link selection.
- Spanning tree protocol (STP) to prune links to the CE router. However, this method requires the service provider to trust its customer to not cause any Layer 2 loops by misconfiguration.
- Active and standby up link functionality, such as the redundant trunk groups that are supported on Juniper Networks EX Series Ethernet Switches.

The limitations of using STP on the CE site are:

- Backbone and access network bandwidth is not used efficiently.
- PE routers using STP to prevent loops with dual-homed sites receive broadcast traffic unnecessarily because the pseudowire to the standby PE router still exists.
- When the direct link between the CE and PE router fails, multihoming works fine. When a link connected downstream from the CE router fails, multihoming does not work.

The benefits and properties of the BGP-based solution are:

- BGP path selection does not have the limitations of STP.
- A CE device that is multihomed to multiple PE routers is given the same site ID on all the PE routers it is multihomed to.
- The BGP path selection algorithm selects the router that originates the best advertisement as the VPLS PE designated forwarder.
- If desired, you can set the local preference on the PE routers to control BGP path selection.
- BGP path selection occurs on the route reflector and the PE router.
- An IGP metric is not part of the selection process.
- If the route distinguisher is the same on both PE routers, the route reflector selects one PE router as the designated forwarder. If the route distinguishers are different on the PE routers, the route reflector forwards both copies of the route to the remote PE routers.

**Related  
Documentation**

- [Example: Next-Generation VPLS for Multicast with Multihoming on page 787](#)
- [Example: NG-VPLS Using Point-to-Multipoint LSPs on page 815](#)
- [Next-Generation VPLS Point-to-Multipoint Forwarding Overview on page 809](#)

## Example: Next-Generation VPLS for Multicast with Multihoming

This example shows how to configure next-generation VPLS for multicast with multihoming. It is organized in the following sections:

- [Requirements on page 787](#)
- [Overview and Topology on page 787](#)
- [Configuration on page 790](#)

### Requirements

The following table lists the hardware and software requirements for this configuration.

**Table 21: Hardware and Software Used**

| Equipment                                                    | Components                                                   | Software                      |
|--------------------------------------------------------------|--------------------------------------------------------------|-------------------------------|
| Four MX Series 3D Universal Edge Routers                     | DPC40X-1GE -X, DPC 4X-10GE-X,<br>DPC40x-1GE-R, DPC 4X-10GE-R | Junos OS Release 9.3 or later |
| Two M320 Multiservice Edge Routers and T Series Core Routers | FPC 3, 10GE Xenpak                                           | Junos OS Release 9.3 or later |
| Five EX Series Ethernet Switches                             | EX4200, EX3200                                               | Junos OS Release 9.4 or later |

### Overview and Topology

[Figure 70 on page 788](#) shows the physical topology used in this next-generation VPLS multihoming example.

**Figure 70: Physical Topology of Next-Generation VPLS for Multicast with Multihoming**

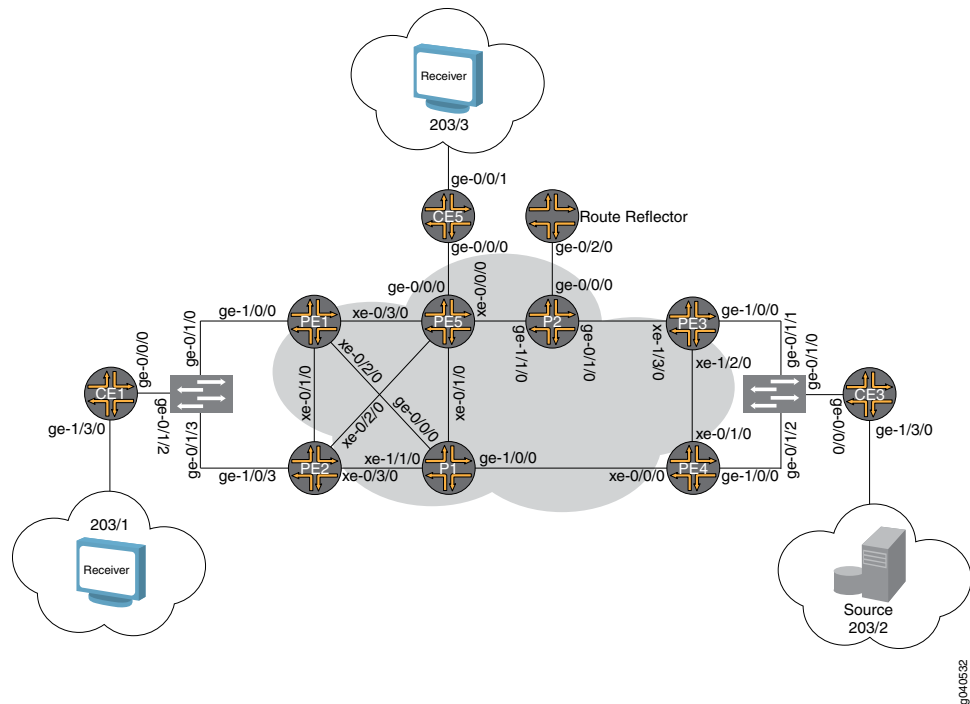
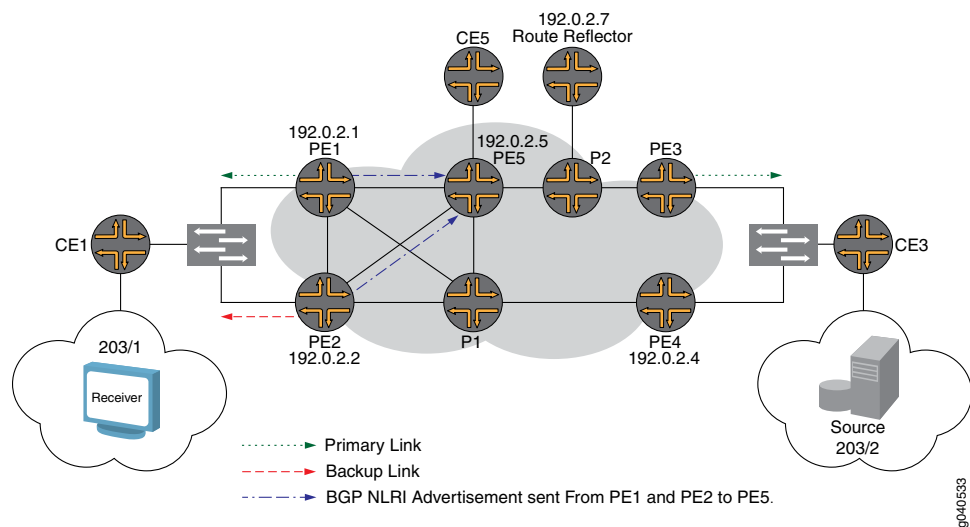


Figure 71 on page 788 show the logical topology of the next-generation VPLS multihoming example.

**Figure 71: Logical Topology of Next-Generation VPLS for Multicast with Multihoming**





The network state and configuration before the implementation is as follows:

- Five PE routers participating in the next-generation VPLS domain named GOLD.
- OSPF, BGP, and RSVP are configured on the MPLS core interfaces.
- The **no-tunnel-services** statement is included in the VPLS routing instance. This statement supports the use of label-switched interface (LSI) tunnel interfaces for VPLS.
- Router PE1 and Router PE2 are configured with a dynamic point-to-multipoint LSP using the **vpls-GOLD-p2mp-template** template.
- Router PE3 and Router PE4 are configured to use static point-to-multipoint LSPs.



**NOTE:** Single-hop point-to-multipoint LSPs are not supported, so single-hop point-to-multipoint LSPs are down.

- Router CE1 is multihomed to Router PE1 and Router PE2 through an EX4200 Layer 2 switch.
- Router CE3 is multihomed to Router PE3 and Router PE4 through an EX4200 Layer 2 switch.
- Router CE5 is singlehomed to Router PE5.
- The off-path route reflector is configured for BGP. The **family l2vpn** statement is included in the route reflector configuration.
- Router CE3 is connected to test equipment through port 203/2. The test equipment generates multicast traffic to groups 203.1.1.1 through 203.1.1.10 at the rate of 10,000 pps.
- Router CE1 and Router CE5 are configured with static Internet Group Management Protocol (IGMP) joins so they can receive the multicast traffic from Router CE3.
- The Layer 2 switches are configured with trunk ports to the PE routers and access ports to the test equipment.

Here is a summary of the steps necessary to complete the configuration successfully:

1. Configure a unique route distinguisher for the VPLS routing instance named GOLD on Router PE1, Router PE2, Router PE3, and Router PE4.
2. Configure the same site ID for the multihomed PE routers. Configure both Router PE1 and Router PE2 with a site ID value of 1. Configure both Router PE3 and Router PE4 with a site ID value of 3.
3. Configure multihoming under the CE1 site configuration.
4. Configure the site-preference **Primary** on Router PE1 and configure the site-preference **Backup** on Router PE2. In this case, Router PE1 has the primary link to Router CE1 and Router PE2 has the backup link to Router CE1.
5. Configure the site preference on Router PE3 and Router PE4. Configure Router PE3 as the primary and Router PE4 as the backup.

## Configuration

This section provides a step-by-step procedure to configure next-generation VPLS for multicast with multihoming.



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

This example is organized in the following sections:

- [Configuring Next-Generation VPLS Multihoming on page 790](#)
- [Validating the VPLS Control Plane on page 792](#)
- [Verifying the VPLS Data Plane on page 798](#)
- [Results on page 801](#)

### Configuring Next-Generation VPLS Multihoming

#### Step-by-Step Procedure

1. In BGP-based VPLS multihoming, it is recommended that you configure distinct route distinguishers for each multihomed router. Configuring distinct route distinguishers helps with faster convergence when the connection to a primary router goes down. It also requires the other backup PE routers to maintain additional state information for faster convergence.

There are two levels of path selection:

- The first is BGP: BGP uses a combination of route distinguisher, site ID, and VE block offset for BGP path selection.
- The second is in VPLS: VPLS uses the site ID for VPLS path selection.

By configuring unique route distinguishers, the prefixes for BGP path selection are all unique. Therefore, BGP path selection is skipped and VPLS path selection is used, which only looks at the site ID.

On Router PE1, Router PE2, Router PE3, and Router PE4 configure a unique router distinguisher for the **GOLD** routing instance.

```
user@PE1# set routing-instance GOLD route-distinguisher 192.0.2.1:1
```

```
user@PE2# set routing-instance GOLD route-distinguisher 192.0.2.2:10
```

```
user@PE3# set routing-instance GOLD route-distinguisher 192.0.2.3:1
```

```
user@PE4# set routing-instance GOLD route-distinguisher 192.0.2.4:10
```

2. Configure site ID 1 on Routers PE1 and PE2 for Router CE1. Configure site ID 3 on Routers PE3 and PE4 for Router CE3.

```
user@PE1# set routing-instance GOLD protocols vpls site CE1 site-identifier 1
```

```
user@PE2# set routing-instance GOLD protocols vpls site CE1 site-identifier 1
```

```
user@PE3# set routing-instance GOLD protocols vpls site CE3 site-identifier 3
```

```
user@PE4# set routing-instance GOLD protocols vpls site CE3 site-identifier 3
```

3. Enable multihoming by including the **multi-homing** statement under the multihomed site configuration on Router PE1, Router PE2, Router PE3, and Router PE4.

```
user@PE1# set routing-instance GOLD protocols vpls site CE1 multi-homing
```

```
user@PE2# set routing-instance GOLD protocols vpls site CE1 multi-homing
```

```
user@PE3# set routing-instance GOLD protocols vpls site CE3 multi-homing
```

```
user@PE4# set routing-instance GOLD protocols vpls site CE3 multi-homing
```

4. Include the **site-preference primary** statement on Router PE1 and Router PE3, and include the **site-preference backup** statement on Router PE2 and Router PE4. The **site-preference primary** statement sets the local preference to the highest value (65535) and the **site-preference backup** statement sets the BGP local preference to 1. Since the site ID is the same, the routers select the highest local preference value as the designated forwarder.

```
user@PE1# set routing-instance GOLD protocols vpls site CE1 site-preference primary
```

```
user@PE2# set routing-instance GOLD protocols vpls site CE1 site-preference backup
```

```
user@PE3# set routing-instance GOLD protocols vpls site CE3 site-preference
primary
```

```
user@PE4# set routing-instance GOLD protocols vpls site CE3 site-preference
backup
```

### Validating the VPLS Control Plane

---

**Step-by-Step Procedure** This section presents show commands that you can use to verify the operation of the example configuration.

In this example the traffic patterns are:

- The source is connected to Router CE3 and sends 10,000 pps for the groups 203.1.1.1 to 203.1.1.10. Router CE3 is configured as a rendezvous point.
- Multicast receivers are connected to both Router CE1 and Router CE5. Protocol Independent Multicast (PIM) join messages are generated by the test equipment.
- The link between Router PE3 and Router CE3 and the link between Router PE1 and Router CE1 are configured as primaries for VPLS multihoming.
- All PE routers have a BGP session with the route reflector.
- All PE routers have a label-switched path (LSP) that is created to the route reflector so that the PE routers have a route to the route reflector in the **inet.3** table for route resolution.

1. On Router PE1, use the **show vpls connections** command to verify that the VPLS connections are **Up** between Router PE1 and Router PE3 and between Router PE1 and PE5. Router PE1 is the primary link selected by the VPLS multihoming configuration.

```
user@PE1# show vpls connections
Layer-2 VPN connections:
```

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -> -- only outbound connection is up           |
| CN -- circuit not provisioned    | <- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unknown connection status  | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not available              |
| BK -- Backup connection          | ST -- Standby connection                       |

Legend for interface status

Up -- operational  
Dn -- down

Instance: GOLD

Local site: CE1 (1)

| connection-site                                               | Type | St | Time last up         | # Up trans |
|---------------------------------------------------------------|------|----|----------------------|------------|
| 1                                                             | rmt  | RN |                      |            |
| 3                                                             | rmt  | Up | Nov 16 11:22:44 2009 | 1          |
| Remote PE: 192.0.2.3, Negotiated control-word: No             |      |    |                      |            |
| Incoming label: 262147, Outgoing label: 262145                |      |    |                      |            |
| Local interface: lsi.1048835, Status: Up, Encapsulation: VPLS |      |    |                      |            |
| Description: Intf - vpls GOLD local site 1 remote site 3      |      |    |                      |            |
| 5                                                             | rmt  | Up | Nov 16 11:22:46 2009 | 1          |
| Remote PE: 192.0.2.5, Negotiated control-word: No             |      |    |                      |            |
| Incoming label: 262149, Outgoing label: 262161                |      |    |                      |            |
| Local interface: lsi.1048836, Status: Up, Encapsulation: VPLS |      |    |                      |            |
| Description: Intf - vpls GOLD local site 1 remote site 5      |      |    |                      |            |

2. On Router PE2, use the **show vpls connections** command to verify that the VPLS connections to Router PE3 and Router PE5 are in the **LN** state, meaning the local router is not the designated forwarder. Router PE2 is configured to be the backup link for Router CE1.

```
user@PE2# show vpls connections
...
```

Instance: GOLD

Local site: CE1 (1)

| connection-site | Type | St | Time last up | # Up trans |
|-----------------|------|----|--------------|------------|
| 1               | rmt  | LN |              |            |
| 3               | rmt  | LN |              |            |
| 5               | rmt  | LN |              |            |

- On Router PE3, use the **show vpls connections** command to verify that the VPLS connections to Router PE1 and Router PE5 are **Up**. Router PE3 is configured to be the primary link for Router CE3.

```
user@PE3# show vpls connections
```

```
...
```

```
Instance: GOLD
```

```
Local site: CE3 (3)
```

| connection-site                                               | Type | St | Time last up         | # Up trans |
|---------------------------------------------------------------|------|----|----------------------|------------|
| 1                                                             | rmt  | Up | Nov 16 11:22:01 2009 | 1          |
| Remote PE: 192.0.2.1, Negotiated control-word: No             |      |    |                      |            |
| Incoming label: 262145, Outgoing label: 262147                |      |    |                      |            |
| Local interface: lsi.1048832, Status: Up, Encapsulation: VPLS |      |    |                      |            |
| Description: Intf - vpls GOLD local site 3 remote site 1      |      |    |                      |            |
| 3                                                             | rmt  | RN |                      |            |
| 5                                                             | rmt  | Up | Nov 16 11:22:56 2009 | 1          |
| Remote PE: 192.0.2.5, Negotiated control-word: No             |      |    |                      |            |
| Incoming label: 262149, Outgoing label: 262163                |      |    |                      |            |
| Local interface: lsi.1048834, Status: Up, Encapsulation: VPLS |      |    |                      |            |
| Description: Intf - vpls GOLD local site 3 remote site 5      |      |    |                      |            |

- On Router PE4, use the **show vpls connections** command to verify that the VPLS connections are in the **LN** state, meaning the local site is not designated. Router PE4 is configured to be the backup link for Router CE3.

```
user@PE4# show vpls connections
```

```
...
```

```
Instance: GOLD
```

```
Local site: CE3 (3)
```

| connection-site | Type | St | Time last up | # Up trans |
|-----------------|------|----|--------------|------------|
| 1               | rmt  | LN |              |            |
| 3               | rmt  | SC |              |            |
| 5               | rmt  | LN |              |            |

- On Router PE1, use the **show route advertising-protocol bgp 192.0.2.7 extensive** command to verify that Router PE1 (the multihoming primary router) is sending the BGP Layer 2 VPN route advertisement to the route reflector with the local preference value of **65535**. The local preference is used by Router PE3 to select Router PE1 as the designated forwarder, rather than selecting Router PE2 that has a local preference of 1.

```
user@PE1# show route advertising-protocol bgp 192.0.2.7 extensive
```

```
GOLD.l2vpn.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
```

```
* 192.0.2.1:1:1:1/96 (1 entry, 1 announced)
```

```
BGP group to-RR type Internal
```

```
Route Distinguisher: 192.0.2.1:1
```

```
Label-base: 262145, range: 8
```

```
Nexthop: Self
```

```
Flags: Nexthop Change
```

```
Localpref: 65535
```

```
AS path: [65000] I
```

```
Communities: target:65000:1 Layer2-info: encaps:VPLS, control flags:, mtu: 0, site preference: 65535
```

```
PMSI: Flags 0:RSVP-TE:label[0:0:0]:Session_13[192.0.2.1:0:9519:192.0.2.1]
```

- On Router PE2, use the **show route advertising-protocol bgp 192.0.2.7 extensive** command to verify that Router PE2 is configured as the multihoming backup with a local preference of 1.

```
user@PE2# show route advertising-protocol bgp 192.0.2.7 extensive
```

GOLD.l2vpn.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

\* 192.0.2.2:10:1:1/96 (1 entry, 1 announced)

BGP group to-RR type Internal

Route Distinguisher: 192.0.2.2:10

Label-base: 262145, range: 8

Nexthop: Self

Flags: Nexthop Change

Localpref: 1

AS path: [65000] I

Communities: target:65000:1 Layer2-info: encaps:VPLS, control flags:, mtu: 0, site preference: 1

7. On Router PE3, use the **show route receive-protocol** command to verify that Router PE3 receives the Layer 2 VPN route from the route reflector for Router PE1 and Router PE2 with different local preference values.

BGP route selection is based on the received **l2vpn** routes for the VPLS site connected to multihomed PE routers. Since the route distinguishers are different on Router PE1 and Router PE2, Router PE3 and Router PE4 consider the received routes from Router PE1 and Router PE2 as different routes. Router PE3 and Router PE4 run the BGP path selection algorithm and select Router PE1, the router advertising the route with the higher local preference value, as the designated forwarder.

user@PE3# **show route receive-protocol bgp 192.0.2.7**

bgp.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)

| Prefix                | Nexthop   | MED | Lc1pref | AS path |
|-----------------------|-----------|-----|---------|---------|
| 192.0.2.1:1:1/96      |           |     |         |         |
| * 192.0.2.2:10:1:1/96 | 192.0.2.1 |     | 65535   | I       |
| * 192.0.2.2:10:1:1/96 | 192.0.2.2 |     | 1       | I       |
| * 192.0.2.4:10:3:1/96 | 192.0.2.4 |     | 1       | I       |
| * 192.0.2.5:10:5:1/96 | 192.0.2.5 |     | 100     | I       |

GOLD.l2vpn.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

| Prefix                | Nexthop   | MED | Lc1pref | AS path |
|-----------------------|-----------|-----|---------|---------|
| 192.0.2.1:1:1/96      |           |     |         |         |
| * 192.0.2.1:1:1/96    | 192.0.2.1 |     | 65535   | I       |
| * 192.0.2.2:10:1:1/96 | 192.0.2.2 |     | 1       | I       |
| * 192.0.2.4:10:3:1/96 | 192.0.2.4 |     | 1       | I       |
| * 192.0.2.5:10:5:1/96 | 192.0.2.5 |     | 100     | I       |

8. On Router PE3, use the **show route table** command to verify that Router PE3 has selected the static point-to-multipoint LSP from Router PE3 to Router PE1 for forwarding.

Notice that Router PE2 does not have any provider multicast service interface (PMSI) flags because PMSI attributes are not attached.

user@PE3# **show route table GOLD.l2vpn.0 extensive**

GOLD.l2vpn.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

192.0.2.1:1:1/96 (1 entry, 1 announced)

\*BGP Preference: 170/-65536

Route Distinguisher: 192.0.2.1:1

PMSI: Flags 0:RSVP-TE:label[0:0:0]:Session\_13[192.0.2.1:0:9519:192.0.2.1]

```

Next hop type: Indirect
Next-hop reference count: 4
Source: 192.0.2.7
Protocol next hop: 192.0.2.1
Indirect next hop: 2 no-forward
State: <Secondary Active Int Ext>
Local AS: 65000 Peer AS: 65000
Age: 2:30:44 Metric2: 1
Task: BGP_65000.192.0.2.7+179
Announcement bits (1): 0-GOLD-12vpn
AS path: I (Originator) Cluster list: 192.0.2.7
AS path: Originator ID: 192.0.2.1
Communities: target:65000:1 Layer2-info: encaps:VPLS, control flags:, mtu: 0, site
preference: 65535
 Import Accepted
 Label-base: 262145, range: 8
 Localpref: 65535
 Router ID: 192.0.2.7
 Primary Routing Table bgp.12vpn.0
 Indirect next hops: 1
 Protocol next hop: 192.0.2.1 Metric: 3
 Indirect next hop: 2 no-forward
 Indirect path forwarding next hops: 1
 Next hop type: Router
 Next hop: 10.10.8.2 via xe-0/1/0.0 weight 0x1
 192.0.2.1/24 Originating RIB: inet.3
 Metric: 3 Node path count: 1
 Forwarding nexthops: 1
 Nexthop: 10.10.8.2 via xe-0/1/0.0

192.0.2.2:10:1:1/96 (1 entry, 1 announced)
 *BGP Preference: 170/-2
 Route Distinguisher: 192.0.2.2:10
 Next hop type: Indirect
 Next-hop reference count: 3
 Source: 192.0.2.7
 Protocol next hop: 192.0.2.2
 Indirect next hop: 2 no-forward
 State: <Secondary Active Int Ext>
 Local AS: 65000 Peer AS: 65000
 Age: 2:30:44 Metric2: 1
 Task: BGP_65000.192.0.2.7+179
 Announcement bits (1): 0-GOLD-12vpn
 AS path: I (Originator) Cluster list: 192.0.2.7
 AS path: Originator ID: 192.0.2.2
 Communities: target:65000:1 Layer2-info: encaps:VPLS, control flags:, mtu: 0, site
preference: 1
 Import Accepted
 Label-base: 262145, range: 8
 Localpref: 1
 Router ID: 192.0.2.7
 Primary Routing Table bgp.12vpn.0
 Indirect next hops: 1
 Protocol next hop: 192.0.2.2 Metric: 3
 Indirect next hop: 2 no-forward
 Indirect path forwarding next hops: 1
 Next hop type: Router
 Next hop: 10.10.8.2 via xe-0/1/0.0 weight 0x1
 192.0.2.2/24 Originating RIB: inet.3
 Metric: 3 Node path count: 1

```



```
Forwarding nexthops: 1
 Nexthop: 10.10.8.2 via xe-0/1/0.0
```

9. On Router PE3, use the **show vpls connections** command to verify that the VPLS connection is in the **Up** state.

Notice the display also shows the local interface and the incoming and outgoing label values used.

```
user@PE3# show vpls connections extensive
```

```
...
```

```
Instance: GOLD
```

```
Local site: CE3 (3)
```

```
Number of local interfaces: 1
```

```
Number of local interfaces up: 1
```

```
IRB interface present: no
```

```
ge-1/0/0.1
```

```
lsi.1048832 1 Intf - vpls GOLD local site 3 remote site 1
```

```
lsi.1048833 2 Intf - vpls GOLD local site 3 remote site 2
```

```
Interface flags: VC-Down
```

```
lsi.1048834 5 Intf - vpls GOLD local site 3 remote site 5
```

```
Interface flags: VC-Down
```

```
Label-base Offset Range Preference
```

```
262145 1 8 65535
```

```
connection-site Type St Time last up # Up trans
```

```
1 rmt Up Nov 16 11:22:01 2009 1
```

```
Remote PE: 192.0.2.1, Negotiated control-word: No
```

```
Incoming label: 262145, Outgoing label: 262147
```

```
Local interface: lsi.1048832, Status: Up, Encapsulation: VPLS
```

```
Description: Intf - vpls GOLD local site 3 remote site 1
```

```
RSVP-TE P2MP lsp:
```

```
Egress branch LSP: 192.0.2.3:192.0.2.1:1:vpls:GOLD, State: Up
```

```
Connection History:
```

```
Nov 16 11:22:54 2009 PE route changed
```

```
Nov 16 11:22:01 2009 status update timer
```

```
Nov 16 11:22:01 2009 PE route changed
```

```
Nov 16 11:22:01 2009 Out lbl Update 262147
```

```
Nov 16 11:22:01 2009 In lbl Update 262145
```

```
Nov 16 11:22:01 2009 loc intf up lsi.1048832
```

```
3 rmt RN
```

```
5 rmt RD
```

```
Ingress RSVP-TE P2MP LSP: vpls-GOLD, Flood next-hop ID: 616
```

## Verifying the VPLS Data Plane

**Step-by-Step Procedure** After the control plane is verified using the previous steps, you can verify the data plane. The data plane operation in the VPLS multihoming scenario is the same as the regular next-generation VPLS operation. This section describes the **show** command outputs that you can use to validate the data plane.

1. On Router PE3, use the **show mpls lsp** command to verify the state of the static LSPs and sub-LSPs.

Router PE2 is configured with static point-to-multipoint LSPs and sub-LSPs with link protection. Point to multipoint LSPs are not supported for single-hop LSPs. In the following output notice that the single-hop point-to-multipoint LSP from Router PE3 to Router PE4 is **down**.

```
user@PE3# show mpls lsp p2mp ingress
Ingress LSP: 1 sessions
P2MP name: vpls-GOLD, P2MP branch count: 4
```

| To        | From      | State | Rt | P | ActivePath | LSPname |
|-----------|-----------|-------|----|---|------------|---------|
| 192.0.2.5 | 192.0.2.3 | Up    | 0  | * |            | to-pe5  |
| 192.0.2.1 | 192.0.2.3 | Up    | 0  | * |            | to-pe1  |
| 192.0.2.4 | 192.0.2.3 | Dn    | 0  | * |            | to-pe4  |
| 192.0.2.2 | 192.0.2.3 | Up    | 0  | * |            | to-pe2  |

```
Total 4 displayed, Up 3, Down 1
```

2. On Router PE1, use the **show mpls lsp** command to verify the state of the dynamic LSPs.

Router PE1 is using a dynamic point-to-multipoint LSP template configured with link protection. Notice that the LSP state is **Up** and that link protection is **desired**.

```
user@PE1# show mpls lsp p2mp ingress extensive
Ingress LSP: 1 sessions
P2MP name: 192.0.2.1:1:vpls:GOLD, P2MP branch count: 1

192.0.2.3
 From: 192.0.2.1, State: Up, ActiveRoute: 0, LSPname: 192.0.2.3:192.0.2.1:1:vpls:GOLD
 ActivePath: (primary)
 P2MP name: 192.0.2.1:1:vpls:GOLD
 Link protection desired
 LoadBalance: Random
 Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary State: Up
 Priorities: 7 0
 OptimizeTimer: 50
 SmartOptimizeTimer: 180
 Reoptimization in 45 second(s).
 Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 3)
10.10.3.2 S 10.10.9.2 S 10.10.8.1 S
 Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node 10=SoftPreempt):
 10.10.3.2(Label=488645) 192.0.2.4(flag=0x21) 10.10.9.2(flag=1 Label=299936)
10.10.8.1(Label=262145)
 12 Nov 16 15:38:08.116 CSPF: computation result ignored[314 times]
 11 Nov 16 11:23:44.856 Link-protection Up
 10 Nov 16 11:23:32.696 CSPF: computation result ignored[3 times]
 9 Nov 16 11:22:47.859 Record Route: 10.10.3.2(Label=488645) 192.0.2.4(flag=0x21) 10.10.9.2(flag=1
Label=299936) 10.10.8.1(Label=262145)
 8 Nov 16 11:22:44.910 Record Route: 10.10.3.2(Label=488645) 192.0.2.4(flag=0x20)
10.10.9.2(Label=299936) 10.10.8.1(Label=262145)
```

```

7 Nov 16 11:22:44.910 Up
6 Nov 16 11:22:44.910 10.10.3.1: Down
5 Nov 16 11:22:44.866 Selected as active path
4 Nov 16 11:22:44.864 Record Route: 10.10.3.2(Label=488629) 192.0.2.4(flag=0x20)
10.10.9.2(Label=299920) 10.10.8.1(Label=3)
3 Nov 16 11:22:44.864 Up
2 Nov 16 11:22:44.852 Originate Call
1 Nov 16 11:22:44.852 CSPF: computation result accepted 10.10.3.2 10.10.9.2 10.10.8.1
Created: Mon Nov 16 11:22:45 2009
Total 1 displayed, Up 1, Down 0

```

3. On Router PE3, use the **monitor interface traffic** command to verify the multicast replication behavior for the point-to-multipoint LSP on the designated forwarder Router PE3.

The output shows that 10,000 pps are received on interface **ge-1/0/0** from Router CE3. The traffic has been forwarded to the provider (P) Router P2 and Router PE4 through **xe-0/0/0** and **xe-0/1/0**, respectively. Based on the output, you can determine that a single copy of the packet is being sent to Router P2 and Router PE4.

```

user@PE3> monitor interface traffic
PE3 Seconds: 8 Time: 11:58:40

```

| Interface | Link | Input packets | (pps)  | Output packets | (pps)   |
|-----------|------|---------------|--------|----------------|---------|
| lc-0/0/0  | Up   | 0             |        | 0              |         |
| xe-0/0/0  | Up   | 13570505      | (0)    | 4507338866     | (10000) |
| lc-0/1/0  | Up   | 0             |        | 0              |         |
| xe-0/1/0  | Up   | 292843        | (1)    | 628972219      | (10000) |
| lc-0/2/0  | Up   | 0             |        | 0              |         |
| xe-0/2/0  | Up   | 343292        | (0)    | 206808         | (1)     |
| lc-0/3/0  | Up   | 0             |        | 0              |         |
| xe-0/3/0  | Down | 0             | (0)    | 0              | (0)     |
| ge-1/0/0  | Up   | 2703709733    | (9999) | 13203544       | (1)     |
| lc-1/0/0  | Up   | 0             |        | 0              |         |
| ge-1/0/1  | Down | 50380341937   | (0)    | 60024542111    | (0)     |
| ge-1/0/2  | Down | 60652323068   | (0)    | 84480825838    | (0)     |
| ge-1/0/3  | Down | 81219536264   | (0)    | 84614255165    | (0)     |
| ge-1/0/4  | Down | 54379241112   | (0)    | 83656815208    | (0)     |

4. On Router P2, use the **monitor interface traffic** command to verify that the multicast packet replication happens close to the PE routers connected to the receivers.

Router PE1 and Router PE5 are connected to receivers that have joined this multicast group. Notice that incoming multicast packets from Router PE3 on the **ge-0/1/0** interface are replicated twice and sent out on the **ge-1/1/0** interface.

```

user@P2> monitor interface traffic
P2 Seconds: 6 Time: 12:07:58

```

| Interface | Link | Input packets | (pps)   | Output packets | (pps)   |
|-----------|------|---------------|---------|----------------|---------|
| ge-0/1/0  | Up   | 661459806     | (10000) | 116236         | (0)     |
| ge-1/1/0  | Up   | 115956        | (0)     | 1322690473     | (20000) |
| gr-2/1/0  | Up   | 0             | (0)     | 0              | (0)     |
| ip-2/1/0  | Up   | 0             | (0)     | 0              | (0)     |

5. On Router PE3, use the **show vpls flood** command to verify information about the flood next-hop route.

Junos OS Release 9.0 and later identifies the flood next-hop route as a composite next hop. Notice that the interface is **ge-1/0/0.1**, the next-hop type is **composite**, and that the flood composition is **flood-to-all**. This means the traffic is flooded to all the PE routers.

```
user@PE3# show vpls flood extensive
```

```
Name: GOLD
```

```
CEs: 1
```

```
VEs: 1
```

```
Flood route prefix: 0x30002/51
```

```
Flood route type: FLOOD_GRP_COMP_NH
```

```
Flood route owner: __ves__
```

```
Flood group name: __ves__
```

```
Flood group index: 0
```

```
Nexthop type: comp
```

```
Nexthop index: 606
```

```
Flooding to:
```

| Name                       | Type  | NhType | Index |
|----------------------------|-------|--------|-------|
| __all_ces__                | Group | comp   | 603   |
| Composition: split-horizon |       |        |       |
| Flooding to:               |       |        |       |
| Name                       | Type  | NhType | Index |
| ge-1/0/0.1                 | CE    | ucst   | 578   |

```
Flood route prefix: 0x30003/51
```

```
Flood route type: FLOOD_GRP_COMP_NH
```

```
Flood route owner: __all_ces__
```

```
Flood group name: __all_ces__
```

```
Flood group index: 1
```

```
Nexthop type: comp
```

```
Nexthop index: 611
```

```
Flooding to:
```

| Name                      | Type  | NhType | Index |
|---------------------------|-------|--------|-------|
| __ves__                   | Group | comp   | 594   |
| Composition: flood-to-all |       |        |       |

```
Component p2mp NH (for all core facing interfaces):
```

```
Index
```

```
616
```

```
Flooding to:
```

| Name                       | Type  | NhType | Index |
|----------------------------|-------|--------|-------|
| __all_ces__                | Group | comp   | 603   |
| Composition: split-horizon |       |        |       |
| Flooding to:               |       |        |       |
| Name                       | Type  | NhType | Index |
| ge-1/0/0.1                 | CE    | ucst   | 578   |

```
Flood route prefix: 0x30001/51
```

```
Flood route type: FLOOD_GRP_COMP_NH
```

```
Flood route owner: __re_flood__
```

```
Flood group name: __re_flood__
```

```
Flood group index: 65534
```

```
Nexthop type: comp
```

```
Nexthop index: 598
```

```
Flooding to:
```

| Name                      | Type  | NhType | Index |
|---------------------------|-------|--------|-------|
| __ves__                   | Group | comp   | 594   |
| Composition: flood-to-all |       |        |       |

```
Component p2mp NH (for all core facing interfaces):
```

```
Index
```

```
616
```

```

Flooding to:
Name Type NhType Index
__all_ces__ Group comp 603
Composition: split-horizon
Flooding to:
Name Type NhType Index
ge-1/0/0.1 CE ucst 578
Name: __juniper_private1__
CEs: 0
VEs: 0

```

6. On Router PE3, use the **show vpls mac-table** command to verify that the MAC address of the PE router at the remote end of the VPLS has been learned and added to the MAC address table.

Notice that the MAC address is learned on the **ge-1/0/0.1** interface.

```

user@PE3# show vpls mac-table
MAC flags (S -static MAC, D -dynamic MAC,
SE -Statistics enabled, NM -Non configured MAC)

```

```

Routing instance : GOLD
Bridging domain : __GOLD__, VLAN : NA
MAC MAC Logical
address flags interface
00:14:f6:75:78:00 D ge-1/0/0.1

```

7. On Router PE3, use the **show route forwarding-table** command to verify that the forwarding table has the required entries with two labels: one for the VPLS service and the other for the next-hop interface.

```

user@PE3> show route forwarding-table family vpls vpn GOLD
Routing table: GOLD.vpls
VPLS:
Destination Type RtRef Next hop Type Index NhRef Netif
default perm 0 dscd 574 1
1si.1048832 intf 0 indr 1048575 4
 10.10.7.1 Push 262147, Push 309680(top) 596 2 xe-0/0/0.0
1si.1048836 intf 0 indr 1048574 4
 10.10.7.1 Push 262179, Push 299856(top) 589 2 xe-0/0/0.0
00:10:db:e9:4e:b6/48
 user 0 indr 1048574 4
 10.10.7.1 Push 262179, Push 299856(top) 589 2 xe-0/0/0.0
00:12:1e:c6:98:00/48
 user 0 indr 1048575 4
 10.10.7.1 Push 262147, Push 309680(top) 596 2 xe-0/0/0.0
00:14:f6:75:78:00/48
 user 0 ucst 578 4 ge-1/0/0.1
0x30002/51 user 0 comp 606 2
ge-1/0/0.1 intf 0 ucst 578 4 ge-1/0/0.1
0x30003/51 user 0 comp 611 2
0x30001/51 user 0 comp 598 2

```

## 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 PE1 follows:

```
Router PE1 chassis {
 dump-on-panic;
 fpc 1 {
 pic 3 {
 tunnel-services {
 bandwidth 1g;
 }
 }
 }
 network-services ethernet;
 }
 interfaces {
 xe-0/1/0 {
 unit 0 {
 family inet {
 address 10.10.2.1/30;
 }
 family mpls;
 }
 }
 xe-0/2/0 {
 unit 0 {
 family inet {
 address 10.10.3.1/30;
 }
 family mpls;
 }
 }
 xe-0/3/0 {
 unit 0 {
 family inet {
 address 10.10.1.1/30;
 }
 family mpls;
 }
 }
 ge-1/0/0 {
 vlan-tagging;
 encapsulation vlan-vpls;
 unit 1 {
 encapsulation vlan-vpls;
 vlan-id 1000;
 family vpls;
 }
 }
 lo0 {
 unit 0 {
 family inet {
 address 192.0.2.1/24;
 }
 }
 }
 }
 routing-options {
 static {
 route 172.0.0.0/8 next-hop 172.19.59.1;
 }
 }
 }
```

```

 }
 autonomous-system 65000;
}
protocols {
 rsvp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 interface xe-0/3/0.0 {
 link-protection;
 }
 interface xe-0/2/0.0 {
 link-protection;
 }
 interface xe-0/1/0.0 {
 link-protection;
 }
 }
}
mpls {
 label-switched-path to-RR {
 to 192.0.2.7;
 }
 label-switched-path vpls-GOLD-p2mp-template {
 template;
 optimize-timer 50;
 link-protection;
 p2mp;
 }
 label-switched-path to-PE2 {
 to 192.0.2.2;
 }
 label-switched-path to-PE3 {
 to 192.0.2.3;
 }
 label-switched-path to-PE4 {
 to 192.0.2.4;
 }
 label-switched-path to-PE5 {
 to 192.0.2.5;
 }
 interface all;
 interface fxp0.0 {
 disable;
 }
}
bgp {
 group to-RR {
 type internal;
 local-address 192.0.2.1;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
}
}

```

```

ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}
}
routing-instances {
 GOLD {
 instance-type vpls;
 interface ge-1/0/0.1;
 route-distinguisher 192.0.2.1:1;
 provider-tunnel {
 rsvp-te {
 label-switched-path-template {
 vpls-GOLD-p2mp-template;
 }
 }
 }
 }
 vrf-target target:65000:1;
 protocols {
 vpls {
 site-range 8;
 no-tunnel-services;
 site CE1 {
 site-identifier 1;
 multi-homing;
 site-preference primary;
 interface ge-1/0/0.1;
 }
 }
 }
}
}

```

The relevant sample configuration for Router PE2 follows.

```

PE2 Router chassis {
 dump-on-panic;
 fpc 1 {
 pic 3 {
 tunnel-services {
 bandwidth 1g;
 }
 }
 }
 network-services ethernet;
 }
 interfaces {
 xe-0/1/0 {
 unit 0 {
 family inet {
 address 10.10.2.2/30;

```



```

 }
 family mpls;
 }
}
xe-0/2/0 {
 unit 0 {
 family inet {
 address 10.10.5.1/30;
 }
 family mpls;
 }
}
xe-0/3/0 {
 unit 0 {
 family inet {
 address 10.10.4.1/30;
 }
 family mpls;
 }
}
ge-1/0/1 {
 vlan-tagging;
 encapsulation vlan-vpls;
}
ge-1/0/3 {
 vlan-tagging;
 encapsulation vlan-vpls;
 unit 1 {
 encapsulation vlan-vpls;
 vlan-id 1000;
 family vpls;
 }
}
fxp0 {
 apply-groups [re0 re1];
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.2/24;
 }
 }
}
}
routing-options {
 static {
 route 172.0.0.0/8 next-hop 172.19.59.1;
 }
 autonomous-system 65000;
}
protocols {
 rsvp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}

```

```
}
mpls {
 label-switched-path to-RR {
 to 192.0.2.7;
 }
 label-switched-path vpls-GOLD-p2mp-template {
 template;
 optimize-timer 50;
 link-protection;
 p2mp;
 }
 label-switched-path to-PE1 {
 to 192.0.2.1;
 }
 label-switched-path to-PE3 {
 to 192.0.2.3;
 }
 label-switched-path to-PE4 {
 to 192.0.2.4;
 }
 label-switched-path to-PE5 {
 to 192.0.2.5;
 }
 interface all;
 interface fxp0.0 {
 disable;
 }
}
bgp {
 group to-RR {
 type internal;
 local-address 192.0.2.2;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
}
ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}
}
routing-instances {
 GOLD {
 instance-type vpls;
 interface ge-1/0/3.1;
 route-distinguisher 192.0.2.2:10;
 provider-tunnel {
 rsvp-te {
 label-switched-path-template {
```

```
 vpls-GOLD-p2mp-template;
 }
}
vrf-target target:65000:1;
protocols {
 vpls {
 site-range 8;
 no-tunnel-services;
 site CE1 {
 site-identifier 1;
 multi-homing;
 site-preference backup;
 interface ge-1/0/3.1;
 }
 }
}
```

**Related  
Documentation**

- [Example: NG-VPLS Using Point-to-Multipoint LSPs on page 815](#)
- [Next-Generation VPLS Point-to-Multipoint Forwarding Overview on page 809](#)
- [Next-Generation VPLS for Multicast with Multihoming Overview on page 781](#)



# Configuring Point-to-Multipoint LSPs

- [Next-Generation VPLS Point-to-Multipoint Forwarding Overview on page 809](#)
- [Example: NG-VPLS Using Point-to-Multipoint LSPs on page 815](#)
- [Flooding Unknown Traffic Using Point-to-Multipoint LSPs in VPLS on page 847](#)
- [Example: Configuring Ingress Replication for IP Multicast Using MBGP MVPNs on page 851](#)
- [Mapping VPLS Traffic to Specific LSPs on page 864](#)

## Next-Generation VPLS Point-to-Multipoint Forwarding Overview

---

VPLS is a Layer 2 solution for efficiently sending multicast traffic over a multiprotocol label switching (MPLS) core.

VPLS emulates the broadcast domain of a LAN across an MPLS network cloud. Traditional MPLS implementations of VPLS require that all participating ingress provider edge (PE) routers make separate copies of each broadcast or multicast packet to send to all other PE routers that are part of the VPLS site for the same extended LAN. In a large virtual private network (VPN), replication overhead can be significant for each ingress router and its attached core-facing links.

Juniper Networks has several important VPLS enhancements that provide a solution for the replication overhead issue:

- Point-to-multipoint LSP support provides efficient distribution of multicast traffic such as IP-based television (IPTV).
- Multihoming support integrates the path selection capability of BGP with VPLS to allow a customer edge (CE) Ethernet switch to have a backup path across the network.

This document explains the use of point-to-multipoint LSPs in the MPLS core as an alternative to ingress replication. Point-to-multipoint LSPs enable ingress routers to send only one copy of each packet into the MPLS cloud. Each PE router maintains a point-to-multipoint tree so traffic can be efficiently sent to all VPN sites. This process requires the fewest possible replications of the packets and does the replication at the most optimal points in the network.

The benefits of this approach are:

- Conservation of bandwidth
- Increased PE router efficiency
- Improved traffic engineering for flows of flooded traffic
- Manual control or several levels of automatic operation
- Simplified multicast optimization, which is ideal for IPTV or network access wholesale

The Internet Engineering Task Force (IETF) supports two standardized VPLS implementations: *RFC 4761: Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling* and *RFC 4762: Virtual Private LAN Service (VPLS) Using LDP Signaling*.

Juniper Networks has implemented VPLS solutions based on both RFCs. BGP-based VPLS is the superior solution, but LDP-based VPLS is supported for those service providers that have already deployed this alternative.

For a detailed technology overview of LDP-BGP VPLS interworking see *LDP-BGP VPLS Interworking* at <http://www.juniper.net/us/en/local/pdf/whitepapers/2000282-en.pdf>.

## Next-Generation VPLS Point-to-Multipoint Forwarding Applications

VPLS provides a multipoint-to-multipoint Ethernet service that can span one or more metro areas and provides connectivity between multiple sites as if these sites were attached to the same Ethernet LAN.

VPLS uses an IP and MPLS service provider infrastructure. From a service provider's point of view, use of IP and MPLS routing protocols and procedures instead of the Spanning Tree Protocol (STP), and MPLS labels instead of VLAN IDs, significantly improves the scalability of the VPLS service.

### VPLS Protocol Operation

VPLS carries Ethernet traffic across a service provider network, so it must mimic an Ethernet network in some ways. When a PE router configured with a VPLS routing instance receives a packet from a CE device, it first determines whether it knows the destination of the VPLS packet. If it does, it forwards the packet to the appropriate PE router or CE device. If it does not, it broadcasts the packet to all the other PE routers and CE devices that are members of that VPLS routing instance. In both cases, the CE device receiving the packet must be different from the one sending the packet.

When a PE router receives a packet from another PE router, it first determines whether it knows the destination of the VPLS packet. If the destination is known, the PE router either forwards the packet or drops it, depending on whether the destination is a local or remote CE device. The PE router has three options (scenarios):

- If the destination is a local CE device, the PE router forwards the packet to it.
- If the destination is a remote CE device (connected to another PE router), it discards the packet.

- If it cannot determine the destination of the VPLS packet, the PE router floods it to its attached CE devices.

A VPLS can be directly connected to an Ethernet switch. Layer 2 information gathered by an Ethernet switch, such as media access control (MAC) addresses and interface ports, is included in the VPLS routing instance table. However, instead of all VPLS interfaces being physical switch ports, the router allows remote traffic for a VPLS instance to be delivered across an MPLS LSP and arrive on a virtual port. The virtual port emulates a local, physical port. Traffic can be learned, forwarded, or flooded to the virtual port in almost the same way as traffic sent to a local port.

The VPLS routing table is populated with MAC addresses and interface information for both physical and virtual ports. One difference between a physical port and a virtual port is that on a virtual port, the router captures the outgoing MPLS label used to reach the remote site and an incoming MPLS label for VPLS traffic received from the remote site. The virtual port is generated dynamically on a Tunnel Services PIC when you configure VPLS on a Juniper Networks M Series Multiservice Edge Router or T Series Core Router. A Tunnel Services PIC is required on each M Series or T Series VPLS router.

If your router has an Enhanced FPC installed, you can configure VPLS without a Tunnel Services PIC. To do so, you use a label-switched interface (LSI) to provide VPLS functionality. An LSI MPLS label is used as the inner label for VPLS. This label maps to a VPLS routing instance. On the PE router, the LSI label is stripped and then mapped to a logical LSI interface. The Layer 2 Ethernet frame is then forwarded using the LSI interface to the correct VPLS routing instance. To configure VPLS on a router without a Tunnel Services PIC, include the **no-tunnel-services** statement.

One restriction on flooding behavior in VPLS is that traffic received from remote PE routers is never forwarded to other PE routers. This restriction helps prevent loops in the core network. This also means that the core network of PE routers must be fully meshed. Additionally, if a CE Ethernet switch has two or more connections to the same PE router, you must enable the Spanning Tree Protocol (STP) on the CE switch to prevent loops.

### Point-to-Multipoint Implementation

In next-generation VPLS, point-to-multipoint LSPs are used to flood broadcast, multicast, and unknown unicast traffic across a VPLS core network to all the PE routers. This is more efficient in terms of bandwidth utilization between the PE router and provider (P) router.

If point-to-multipoint LSPs are not being used, the PE router needs to forward multiple copies of broadcast, multicast, and unknown unicast packets to all PE routers. If point-to-multipoint LSPs are used, the PE router floods one copy of each packet to the P router, where it is replicated close to the egress router.



**NOTE:** For next-generation VPLS, both point-to-point LSPs and point-to-multipoint LSPs are needed between the PE routers.

In VPLS, point-to-multipoint LSPs are only used to transport broadcast frames, multicast frames, and unicast frames with an unknown destination MAC address. All other frames are still transported using point-to-point LSPs. This structure is much more efficient for bandwidth use, particularly near the source of the broadcast, multicast, and unknown frames. However, it also results in more state in the network because each PE router is the ingress of one point-to-multipoint LSP that touches all other PE routers and one point-to-point LSP going to each of the other PE routers.

Enabling point-to-multipoint LSPs for any VPLS instance starts the flooding of unknown-unicast, broadcast, and multicast traffic using point-to-multipoint LSPs.

For each VPLS instance, a PE router creates a dedicated point-to-multipoint LSP. Whenever VPLS discovers a new neighbor through BGP, a source-to-leaf sub-LSP is added for this neighbor in the point-to-multipoint LSP instance.

If there are  $n$  PE routers in the VPLS instance, then the discovery of a new neighbor through BGP creates  $n$  point-to-multipoint LSPs in the network, where each PE router is the root of the tree and the rest of the  $n-1$  PE routers are leaf nodes (or source-to-leaf sub-LSPs).

Each point-to-multipoint LSP created by PE routers can be identified using an RSVP-traffic engineering point-to-multipoint session object, which is passed as a provider multicast service interface (PMSI) tunnel attribute by BGP while advertising VPLS routes. Using this tunnel attribute, incoming source-to-leaf sub-LSP add request messages (RSVP-path message) can be associated with the right VPLS instance and originator PE router. As a result, label allocation is done in such a way that when traffic arrives on the LSP, it is not only terminated on the right VPLS instance, but the originator PE router is also identified so that source MAC addresses can be learned.

Point-to-multipoint LSPs can be enabled incrementally on any PE router that is part of a specific VPLS instance. This means a PE router that has this feature uses point-to-multipoint LSPs to flood traffic, whereas other PE routers in the same VPLS instance can use ingress replication to flood the traffic. However, when point-to-multipoint LSPs are enabled on any PE router, make sure that all the PE routers that are part of the same VPLS instance also support this feature.



**NOTE:** Penultimate-hop popping (PHP) is disabled for point-to-multipoint LSPs terminating in a VPLS instance.

---

### Limitations of Point-to-Multipoint LSPs

When implementing point-to-multipoint LSPs remember the following limitations:

- There is no mechanism to allow only multicast traffic to go over the point-to-multipoint LSP.
- Point-to-multipoint LSPs do not support inter-AS traffic. Only intra-AS traffic is supported.
- Point-to-multipoint LSPs do not support graceful restart for ingress LSPs. This also affects VPLS when flooding is done using point-to-multipoint LSPs.



- The same point-to-multipoint LSP cannot be shared across multiple VPLS instances.
- When this feature is enabled, ingress PE routers use only point-to-multipoint LSPs for flooding. The router initiates the creation of source-to-leaf sub-LSPs for each PE router that is part of the same VPLS instance. Any PE router for which this source-to-leaf sub-LSP fails to come up does not receive any flooded traffic from the ingress PE router.
- It is possible that flooding of unknown unicast traffic over point-to-multipoint LSPs may lead to packet reordering, because as soon as learning is done, unicast traffic is sent out using point-to-point pseudowire LSPs.
- Static LSPs and LSPs configured using the **label-switched-path-template** statement cannot be configured at the same time.
- When an LSP is configured using the **static-lsp** statement, a point-to-multipoint LSP is created statically to include all neighbors in the VPLS instance.

Before enabling the point-to-multipoint LSP feature on any PE router, make sure that all the other PE routers that are part of the same VPLS instance are upgraded to a Junos OS Release that supports it. If a router in the VPLS instance does not support point-to-multipoint LSPs, it may lose all the traffic sent on the point-to-multipoint LSP. Therefore, do not enable this feature if there is a single router in a VPLS instance that is not capable of supporting this feature, either because it is not running the appropriate Junos OS Release or because it is a router from a vendor that does not support this feature.

### Simultaneous Transit and Egress Router Operation

A PE router that plays the role of both an MPLS transit router and an MPLS egress router can do so by receiving either one or two copies of a packet to fulfill each of its roles.

To fulfill both roles while using only a single copy of a packet, Juniper Networks M Series and T Series routers require a Tunnel Services PIC configured with virtual tunnel (vt) interfaces and ultimate-hop popping must be enabled. With a virtual tunnel interface and ultimate-hop popping, a single copy of the received packet is forwarded beyond the PE router to fulfill the transit router role and is also consumed internally by the virtual tunnel interface to fulfill the egress router role.

If a label-switched interface (LSI) logical interface is used, then two copies of each packet must be received on the point-to-multipoint LSP, one to fulfill the transit router role and one to fulfill the egress router role.

## Implementation

Some implementations of VPLS use ingress replication. Ingress replication is simple but inefficient. It sends multiple copies of the same packet on a link, especially the PE-P link. This causes wasted bandwidth when there is a heavy broadcast and multicast traffic.

As shown in the sample network in [Figure 72 on page 814](#) the ingress PE router makes three copies of every broadcast, multicast, and flooded packet for each VPLS instance.

Figure 72: Ingress Replication

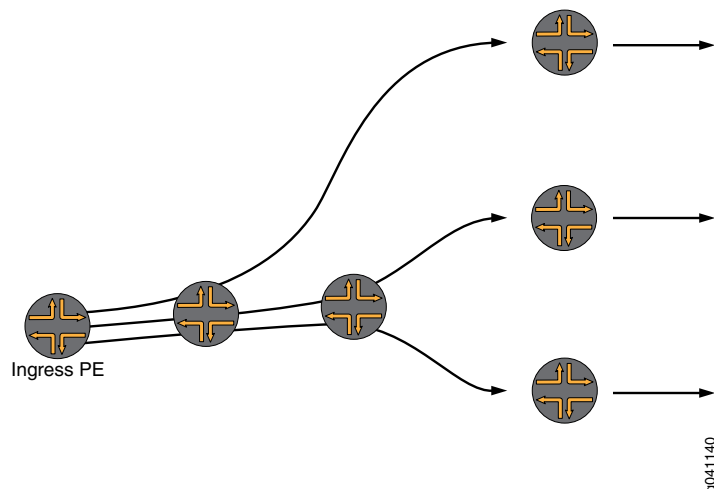
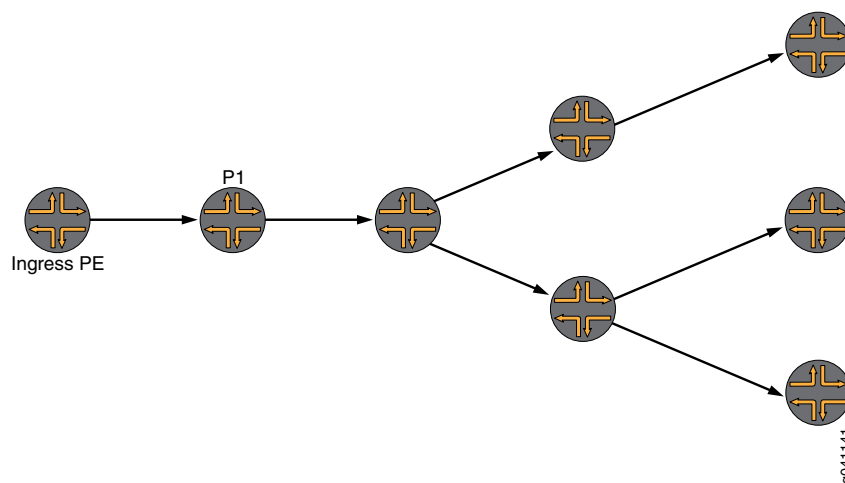


Figure 73 on page 814 shows how a point-to-multipoint LSP works for multicast.

In a VPLS using point-to-multipoint LSPs, the ingress PE router sends a single copy of the multicast packet to Router P1. Router P1 makes two copies for this point-to-multipoint LSP. Each of the other P routers also makes multiple copies of the packet. This moves replication closer to the endpoints and results in significant improvements in the network bandwidth utilization.

Figure 73: Point-to-Multipoint Replication



**Related Documentation**

- [Example: NG-VPLS Using Point-to-Multipoint LSPs on page 815](#)

## Example: NG-VPLS Using Point-to-Multipoint LSPs

This example shows how to configure next-generation VPLS (NG\_VPLS) using point-to-multipoint LSPs. The topology is shown in [Figure 74 on page 816](#) and [Figure 75 on page 817](#). This example is organized in the following sections:

- [Requirements on page 815](#)
- [Overview and Topology on page 815](#)
- [Configuration on page 818](#)

### Requirements

[Table 22 on page 815](#) lists the hardware that is used and the software that is required for this example:

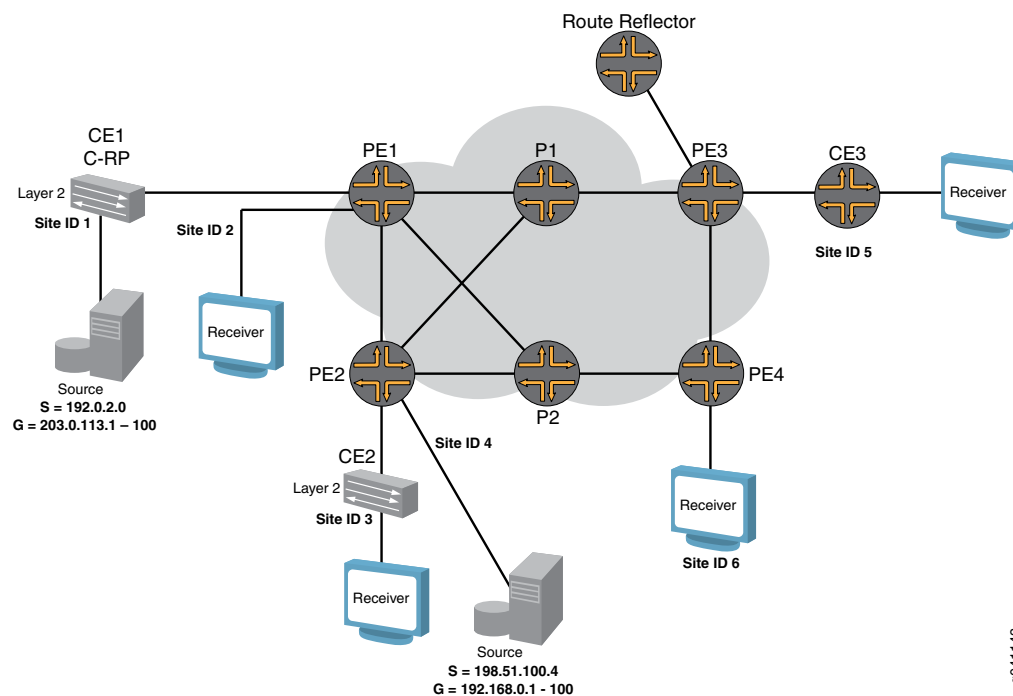
**Table 22: Hardware and Software Used**

| Equipment                               | Components                  | Software                        |
|-----------------------------------------|-----------------------------|---------------------------------|
| Six MX Series 3D Universal Edge Routers | DPC-4 10GE-X, DPC-40 1GE-X  | Junos OS Release 9.3R4 or later |
| One T Series Core Router                | FPC3, 10GE-Xenpak           | Junos OS Release 9.3R4 or later |
| Eight EX4200 Ethernet Switches          | EX4200 virtual switches     | Junos OS Release 9.3R4 or later |
| One M7i Multiservice Edge Router        | Gigabit Ethernet interfaces | Junos OS Release 9.3R4 or later |

### Overview and Topology

The logical topology of the NG-VPLS example is shown in [Figure 74 on page 816](#).

Figure 74: Logical Topology of NG-VPLS Using Point-to-Multipoint LSPs

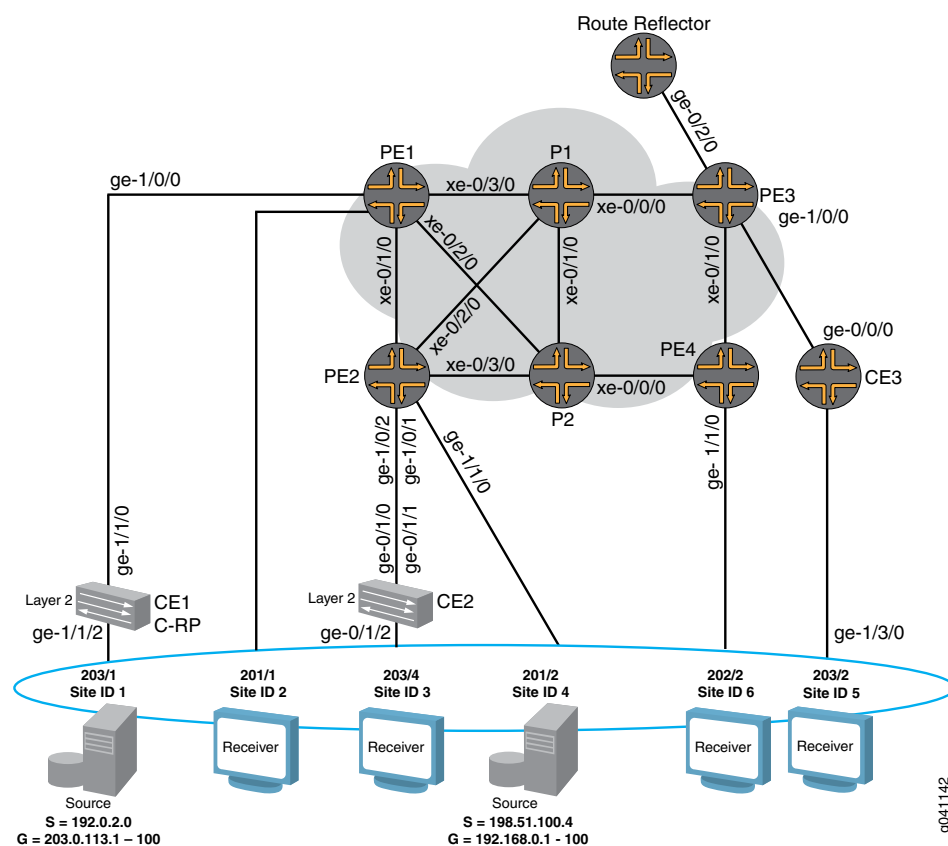


The routers in this example are preconfigured with the following:

- OSPF area 0 is configured on all the PE routers and P routers with traffic engineering enabled.
- All of the core-facing interfaces are configured with the **mpls** protocol address family.
- The RSVP and MPLS protocols are enabled for all the core-facing interfaces.
- All the MX Series routers have their network services mode set to Ethernet. The network services mode is configured by including the **network-services** statement and specifying the **ethernet** option.
- All the PE routers are configured for autonomous system **65000**.

The physical topology of the NG-VPLS example is shown in [Figure 75 on page 817](#). The topology consists of six MX Series routers connected with redundant links in the core. Four MX Series routers are acting as PE routers and two are core routers.

Figure 75: Physical Topology of NG-VPLS Using Point-to-Multipoint LSPs



Note the following topology details:

- A route reflector is configured in the topology to reflect the family **l2-vpn** routes to all the PE routers for BPG-VPLS.
- The GOLD VPLS routing instance is configured with two sites in each of the PE routers.
- One GOLD site is connected to the CE router and the other one is directly connected to the test equipment on each PE router.
- The **no-tunnel-services** statement is included in the GOLD VPLS instance to enable the use of LSI interfaces for VPLS tunnel services.
- Router CE1 and Router CE2 are EX Series Virtual Chassis switches acting as CE routers.
- Router CE3 is an M7i router acting as a CE router.
- Two multicast sources are configured. One is connected to Router CE1 (Site 1) and the other to Router PE2 (Site 4) to simulate different scenarios.
- Router CE1 is configured as the rendezvous point (RP).
- Unicast traffic is enabled on all the test equipment ports and is sent to all the sites in the GOLD VPLS instance.

## Configuration

This example shows how to configure next-generation VPLS using point-to-multipoint LSPs. It is organized in the following sections:

- [Configuring the PE Router Interfaces on page 818](#)
- [Configuring a Route Reflector for all PE Routers for BGP-Based VPLS on page 820](#)
- [Establishing BGP-Based VPLS with a Route Reflector on page 821](#)
- [Configuring Point-to-Point LSPs Between PE Routers on page 822](#)
- [Configuring Dynamic and Static Point-to-Multipoint LSPs Between PE Routers on page 822](#)
- [Configuring Point-to-Multipoint Link Protection on page 823](#)
- [Configuring a BGP-Based VPLS Routing Instance for NG-VPLS on page 825](#)
- [Configuring Tunnel Services for VPLS on page 828](#)
- [Verifying the Control Plane on page 829](#)
- [Verifying the Data Plane on page 837](#)
- [Results on page 841](#)

---

### Configuring the PE Router Interfaces

#### Step-by-Step Procedure

On the customer-facing PE interfaces, enable VLAN tagging, configure the encapsulation type, and enable the VPLS address family. There are four possible interface encapsulations for VPLS routing instances that you can choose depending on your needs.

1. If your network requires that each logical interface on the PE router-to-CE router link be configured to only accept packets with VLAN ID **1000**, include the **vlan-tagging** statement, include the **encapsulation** statement, and specify **vlan-vpls** as the encapsulation type. Also include the **vlan-id** statement and specify **1000** as the VLAN ID.

```
[edit interfaces]
ge-1/1/0 {
 vlan-tagging;
 encapsulation vlan-vpls;
 unit 1 {
 encapsulation vlan-vpls;
 vlan-id 1000;
 family vpls;
 }
}
```

With this configuration, you can configure multiple logical interfaces with different VLAN IDs and associate each logical interface with a different routing instance.

2. If your network requires each physical interface on the PE router to CE router link to be configured to use the entire Ethernet port as part of a single VPLS instance, include the **encapsulation** statement, and specify **ethernet-vpls** as the encapsulation type.

```
[edit interfaces]
```

```

ge-1/2/0 {
 encapsulation ethernet-vpls;
 unit 0 {
 family vpls;
 }
}

```

With this encapsulation mode, you cannot create multiple logical units (VLANs).

3. If your network requires that each logical interface of the single physical interface on the PE router to CE router link be configured to use a mix of different encapsulations, include the **encapsulation** statement, and specify **flexible-ethernet-services** as the encapsulation type at the **[edit interfaces interface-name]** hierarchy level. Also include the **encapsulation** statement, and specify **vlan-vpls** or **vlan-ccc** as the encapsulation type at the **[edit interfaces interface-name unit logical-unit-number]** hierarchy level.

```

[edit interfaces]
ge-1/2/0 {
 vlan-tagging;
 encapsulation flexible-ethernet-services;
 unit 1 {
 encapsulation vlan-vpls;
 }
 unit 2 {
 encapsulation vlan-ccc;
 }
}

```

4. If your network requires support for using a mix of single and dual tagged VLANs configured in different logical interfaces on a single physical interface, include the **encapsulation** statement, and specify **flexible-vlan-tagging** as the encapsulation type.
5. Configure the core-facing CE router interfaces. The CE router and PE router logical interface configuration must match encapsulation types and VLAN IDs. Typically the IP address is configured on the core-facing CE router interfaces if the CE device is a router and terminates the Layer 2 domain into the Layer 3 network. In this example, the interface is configured for single tagging with a VLAN ID of 1000.

```

[edit interfaces]
ge-1/1/0 {
 vlan-tagging;
 unit 1 {
 vlan-id 1000;
 family inet {
 address 198.51.100.4/24;
 }
 }
}

```

### Configuring a Route Reflector for all PE Routers for BGP-Based VPLS

#### Step-by-Step Procedure

Configuring a route reflector is the preferred method to enable any BGP-based service offerings. Configuring a route reflector avoids the requirement for a full mesh of BGP peer sessions, and it scales well. BGP redundancy can be achieved using multiple route reflectors in a single cluster.

1. To enable BGP to carry Layer 2 VPN and VPLS NLRI messages, create a peer group, include the **family** statement, specify the **l2vpn** option, and include the **signaling** statement. To configure the route reflector cluster and complete the BGP peer sessions, include the **cluster** statement and specify the IP address for the cluster ID. Then include the **neighbor** statement and specify the IP address of the PE routers that are BGP client peers in the cluster.

```
[edit protocols]
bgp {
 group RR {
 type internal;
 local-address 192.0.2.7;
 family l2vpn {
 signaling;
 }
 cluster 192.0.2.7;
 neighbor 192.0.2.1; # To PE1
 neighbor 192.0.2.2; # To PE2
 neighbor 192.0.2.3; # To PE3
 neighbor 192.0.2.4; # To PE4
 }
}
```

2. Configure OSPF and enable traffic engineering on the route reflector to create the Constrained Shortest Path First (CSPF) database for the egress LSPs terminating from the PE routers.

```
[edit protocols]
ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}
```

3. Enable the MPLS and RSVP protocols on all interfaces connected to the MPLS core. This terminates the RSVP egress LSPs from the PE routers.

```
[edit protocols]
rsvp {
 interface all;
 interface fxp0.0 {
 disable;
 }
}
```



```

mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
}

```

### Establishing BGP-Based VPLS with a Route Reflector

#### Step-by-Step Procedure

For BGP-based VPLS, all PE routers need to have a full mesh of BGP peer sessions with each other or have a single peer with the route reflector. The route reflector reflects the routes received from the other PE routers. In this example, the PE router is configured to establish a peer relationship with the route reflector.

1. To have all the PE routers establish a BGP client peer session with the route reflector, create an internal peer group, include the **local-address** statement, and specify the IP address of the PE router. Also include the **neighbor** statement, and specify the IP address of the route reflector. To enable BGP to carry Layer 2 VPN and VPLS NLRI messages, include the **family** statement, specify the **l2vpn** option, and include the **signaling** statement.

```

[edit protocols]
bgp {
 group to-RR {
 type internal;
 local-address 192.0.2.1;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7; # To the route reflector
 }
}

```

2. Configure a point-to-point RSVP LSP from the PE routers to the route reflector. To create the LSP, include the **label-switched-path** statement, give the LSP a meaningful name, include the **to** statement and specify the IP address of the route reflector as the LSP end point. This LSP is needed to resolve the BGP next hops in the **inet.3** routing table for the routes received from the route-reflector.

```

[edit protocols]
mpls {
 label-switched-path to-RR {
 to 192.0.2.7;
 }
 interface all;
 interface fxp0.0 {
 disable;
 }
}

```

### Configuring Point-to-Point LSPs Between PE Routers

**Step-by-Step Procedure** In next-generation VPLS, point-to-multipoint LSPs are only used to transport broadcast, multicast, and unknown unicast frames. All other frames are still transported using point-to-point RSVP LSPs. This is a more efficient use of bandwidth, particularly near the source of the unknown, broadcast, and multicast frames. The trade-off is more state in the network, because each PE router is the ingress of one point-to-multipoint LSP that touches all other PE routers, and  $n$  point-to-point LSPs are needed, one going to each of the other PE routers.

1. To create a point-to-point LSP, include the **label-switched-path** statement, give the LSP a meaningful name, include the **to** statement, and specify the IP address of the other PE router as the LSP endpoint. The example shows the configuration of LSPs from Router PE1 to Routers PE2, PE3, and PE4.

```
[edit protocols]
mpls {
 label-switched-path to-PE2 {
 to 192.0.2.2;
 }
 label-switched-path to-PE3 {
 to 192.0.2.3;
 }
 label-switched-path to-PE4 {
 to 192.0.2.4;
 }
}
```

### Configuring Dynamic and Static Point-to-Multipoint LSPs Between PE Routers

**Step-by-Step Procedure** This procedure describes how to enable the creation of dynamic point-to-multipoint LSPs and how to configure static point-to-multipoint LSPs. On a router configured with static point-to-multipoint LSPs, the LSPs come up immediately. On a router configured with dynamic point-to-multipoint LSPs, the LSP comes up only after receiving BGP neighbor information from the route reflector or from the other PE routers participating in the VPLS domain.

For each VPLS instance, a PE router with dynamic point-to-multipoint LSPs enabled creates a dedicated point-to-multipoint LSP based on the point-to-multipoint template. Whenever VPLS discovers a new neighbor through BGP, a sub-LSP for this neighbor is added to the point-to-multipoint LSP.

If there are  $n$  PE routers in the VPLS instance then the router creates  $n$  point-to-multipoint LSPs in the network where each PE router is the root of the tree and includes the rest of the  $n-1$  PE routers as leaf nodes connected through a source-to-leaf sub-LSP.

1. In this step, you configure Router PE1 and Router PE2 to use a dynamic point-to-multipoint LSP template for LSP creation. When these routers receive a new BGP route advertised from the route reflector for a new neighbor, they create a point-to-multipoint sub-LSP to that neighbor. To create the dynamic point-to-multipoint LSP template, include the **label-switched-path** statement, give the LSP template a meaningful name, include the **template** statement and include

the **p2mp** statement. Also enable link protection and configure the optimize timer to periodically reoptimize the LSP path.

```
[edit protocols]
mpls {
 label-switched-path vpls-GOLD-p2mp-template {
 template; # identify as a template
 optimize-timer 50;
 link-protection; # link protection is enabled on point-to-multipoint LSPs
 p2mp;
 }
}
```

2. In this step, you configure static point-to-multipoint LSPs. Creating static point-to-multipoint LSPs is similar to creating point-to-point LSPs, except you can also configure other RSVP parameters under each point-to-multipoint LSP.

To create static point-to-multipoint LSPs, include the **label-switched-path** statement, give the LSP a meaningful name, include the **to** statement, and specify the IP address of the PE router that is the endpoint of the LSP. Also include the **p2mp** statement and specify a pathname.

```
[edit protocols]
mpls {
 label-switched-path to-pe2 {
 to 192.0.2.2;
 p2mp vpls-GOLD;
 }
 label-switched-path to-pe3 {
 to 192.0.2.3;
 p2mp vpls-GOLD;
 }
 label-switched-path to-pe1 {
 to 192.0.2.1;
 p2mp vpls-GOLD;
 }
}
```

### Configuring Point-to-Multipoint Link Protection

#### Step-by-Step Procedure

Point-to-multipoint LSPs only support RSVP link protection for traffic engineering. Node protection is not supported. Link protection is optional, but it is the recommended configuration for most networks.

1. To enable link protection on the core-facing interfaces, include the **link-protection** statement at the **[edit protocols rsvp interface *interface-name*]** hierarchy level.

```
[edit protocols]
rsvp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 interface xe-0/3/0.0 {
 link-protection;
 }
}
```

```

interface xe-0/2/0.0 {
 link-protection;
}
interface xe-0/1/0.0 {
 link-protection;
}
}

```

2. Enable the point-to-multipoint LSP to use the RSVP link protection feature. Link-protection can be configured for both static point-to-multipoint and dynamic point-to-multipoint LSPs that use a template.

For static point-to-multipoint LSPs, configure each branch sub-LSP. To enable link protection, include the **link-protection** statement at the **[edit protocols mpls label-switched-path *label-switched-path-name*]** hierarchy level.

```

[edit protocols mpls label-switched-path]
label-switched-path to-pe2 {
 to 192.0.2.2;
 link-protection;
 p2mp vpls-GOLD;
}
label-switched-path to-pe3 {
 to 192.0.2.3;
 link-protection;
 p2mp vpls-GOLD;
}
label-switched-path to-pe1 {
 to 192.0.2.1;
 link-protection;
 p2mp vpls-GOLD;
}
}

```

3. For dynamic point-to-multipoint LSPs using a template, only the template needs to have link protection configured. All the point-to-multipoint branch LSPs that use the template inherit this configuration.

To enable link protection for dynamic point-to-multipoint LSPs, include the **link-protection** statement at the **[edit protocols mpls label-switched-path *label-switched-path-name*]** hierarchy level.

```

[edit protocols mpls label-switched-path]
label-switched-path vpls-GOLD-p2mp-template {
 template;
 optimize-timer 50;
 link-protection;
 p2mp;
}

```

### Configuring a BGP-Based VPLS Routing Instance for NG-VPLS

#### Step-by-Step Procedure

For NG-VPLS, the routing-instance configuration is similar to that for a regular VPLS routing instance. The routing instance defines the VPLS site and creates the VPLS connection. The following parameters are configured.

- Instance Type – VPLS.
  - Interface – The interface connecting to the CE router.
  - Route Distinguisher – Each routing instance you configure on a PE router must have a unique route distinguisher. The route distinguisher is used by BGP to distinguish between potentially identical network reachability information (NLRI) messages received from different VPNs. If you use a unique route distinguisher for each routing instance on each PE, you can determine which PE originated the route.
  - VRF Target – Configuring a VRF target community using the **vrf-target** statement causes default VRF import and export policies to be generated that accept imported routes and tag exported routes with the specified target community.
  - Protocols – Configure the VPLS protocol as described in the following procedure.
1. To configure the NG-VPLS routing instance, include the **routing-instances** statement and specify the instance name. Also include the **instance-type** statement and specify **vpls** as the type. Include the **route-distinguisher** statement and specify a route distinguisher that is unique throughout all VPNs configured on the router. Configure a VRF route target by including the **vrf-target** statement and specify the route target. The route target exported by one router must match the route target imported by another router for the same VPLS.

```
[edit]
routing-instances {
 GOLD {
 instance-type vpls;
 interface ge-1/0/0.1;
 interface ge-1/1/0.1;
 route-distinguisher 192.0.2.1;
 vrf-target target:65000:1;
 }
}
```

2. To use a point-to-multipoint LSP for VPLS flooding, configure an LSP under the VPLS routing instance.

To configure the point-to-multipoint LSP for VPLS flooding, include the **label-switched-path-template** statement and specify the name of the LSP template at the **[edit routing-instances routing-instances-name provider-tunnel rsvp-te]** hierarchy level.

```
[edit]
routing-instances {
 GOLD {
 instance-type vpls;
 interface ge-1/0/0.1;
 interface ge-1/1/0.1;
```

```

route-distinguisher 192.0.2.1:1;
provider-tunnel {
 rsvp-te {
 label-switched-path-template {
 vpls-GOLD-p2mp-template;
 }
 }
}
vrf-target target:65000:1;
}
}

```

3. Configuring the VPLS protocol enables the VPLS between different sites in the VPLS domain. Multiple sites can be configured under a single VPLS routing instance, but note that the lowest site ID is used to build the VPLS pseudowire to the other PE routers, and the label block associated with the lowest site ID is advertised. The following parameters are configured for the VPLS protocol:
  - Site – Name of the VPLS site.
  - Site Range – Maximum site ID allowed in the VPLS. The site range specifies the highest-value site ID allowed within the VPLS, not the number of sites in the VPLS.
  - Site Identifier – Any number between 1 and 65,534 that uniquely identifies the VPLS site. This is also referred as the VE-ID in the relevant RFC.
  - PE-CE Interface – The interface participating in this site.
  - Tunnel services for VPLS – If you do not configure any tunnel interface at the **[edit protocol vpls tunnel-services]** hierarchy, the router uses any tunnel interface available on the router for VPLS.
  - No-tunnel-services – If you include the **no-tunnel-services** statement, the router uses a label-switched interface (LSI) for the tunnel services for that VPLS instance.
  - Mac Table Size – The size of the VPLS media access control (MAC) address table. The default is 512 addresses and the maximum is 65,536. When the table is full, new MAC addresses are no longer added to the table.

To configure the VPLS protocol, include the **vpls** statement at the **[edit routing-instances routing-instance-name protocols]** hierarchy level. To configure the site range, include the **site-range** statement and specify the highest-value site ID allowed within the VPLS. To cause the router to use an LSI interface, include the **no-tunnel-services** statement. To create a VPLS site, include the **site** statement and specify a site name. Also include the **site-identifier** statement and specify the site ID. Then include the **interface** statement and specify the interface name for the interface connected to the CE device.

```

[edit]
routing-instances {
 GOLD {
 instance-type vpls;
 interface ge-1/0/0.1;
 interface ge-1/1/0.1;
 route-distinguisher 192.0.2.1:1;
 provider-tunnel {

```

```
 rsvp-te {
 label-switched-path-template {
 vpls-GOLD-p2mp-template;
 }
 }
 }
 vrf-target target:65000:1;
 protocols {
 vpls {
 site-range 8;
 no-tunnel-services;
 site CE1 {
 site-identifier 1;
 interface ge-1/0/0.1;
 }
 site Direct {
 site-identifier 2;
 interface ge-1/1/0.1;
 }
 }
 }
}
```

## Configuring Tunnel Services for VPLS

### Step-by-Step Procedure

A tunnel interface is needed for VPLS configuration to encapsulate the originating traffic, and to de-encapsulate the traffic coming from a remote site. If the tunnel interface is not configured, the router selects one of the available tunnel interfaces on the router by default. There are three methods available in Junos OS to configure this tunnel interface.

- To specify a virtual tunnel interface to be used as the primary device for tunneling, include the **primary** statement, and specify the virtual tunnel interface to be used at the **[edit routing-instances *routing-instance-name* protocols vpls tunnel-services]** hierarchy level.

```
[edit routing-instances routing-instance-name]
protocols {
 vpls {
 site-range 8;
 tunnel-services {
 primary vt-1/2/10;
 }
 }
}
```

- To configure the router to use an LSI interface for tunnel services rather than a virtual tunnel interface, include the **no-tunnel-services** statement at the **[edit routing-instances *routing-instance-name* protocols vpls]** hierarchy level.

```
[edit routing-instances routing-instance-name]
protocols {
 vpls {
 site-range 8;
 no-tunnel-services;
 }
}
```

- In an MX Series router you must create the tunnel services interface to be used for tunnel services. To create the tunnel service interface, include the **bandwidth** statement and specify the amount of bandwidth to reserve for tunnel services in gigabits per second at the **[edit chassis *fpc slot-number* pic *slot-number* tunnel-services]** hierarchy level.

```
[edit chassis]
fpc 1 {
 pic 3 {
 tunnel-services {
 bandwidth 1g;
 }
 }
}
```



### Verifying the Control Plane

---

- Step-by-Step Procedure** This section describes **show** command outputs you can use to validate the control plane. It also provides methodologies for troubleshooting. Note the following:
- In this example there are six sites. Router PE1 and Router PE2 have two sites each. Router PE3 and Router PE4 have one site each. All sites are in the GOLD VPLS instance.
  - In VPLS if you have multiple sites configured under a single VPLS routing instance, the label block from the site with the lowest site ID is used to establish pseudowires between remote PEs. Note that the data traffic is still sent to those PE router interfaces connected to CE devices that are in one of the following states:
    - LM – Local site ID is not the minimum designated. The local site ID is not the lowest. Therefore the local site ID is not being used to establish pseudowires or distribute VPLS label blocks.
    - RM – Remote site ID is not the minimum designated. The remote site ID is not the lowest. Therefore, the remote site ID is not being used to establish pseudowires or distribute VPLS label blocks.
  - For more information about how VPLS label blocks are allocated and used, see *Understanding VPLS Label Blocks Operation*.

1. After the entire configuration is done, you can verify the VPLS connections state.

In the following output, the VPLS connections show the **Up** state for certain sites, and the remaining sites show either the **RM** or **LM** state. This is the expected state in a VPLS implementation on multihoming sites.

In this example, Router PE1 has site **CE1** configured with site ID 1 and site **Direct** configured with site ID 2. The label block for site **CE1** is advertised to the remote PE routers and used for receiving the data packets from the remote PE routers. In the **show** command output, notice the following:

- Router PE1 uses its lowest site ID, which is site ID 1. Site ID 1 is used for Device **CE1**.
- Router PE2 uses its lowest site ID, which is site ID 3. Site ID 3 is used for Device **CE2**.
- Router PE3 and Router PE4 each have a single site configured.

For site **CE1**, connection site 3 is in the **Up** state and connection site 4 is in the **RM** state.

- For site **Direct**, all the connections are in the **LM** state.
- Site **Direct** has a higher site ID than site 1 on this router.

On Router PE1, use the **show vpls connections** command to verify the VPLS connections state.

```
user@PE1> show vpls connections
Layer-2 VPN connections:
```

Legend for connection status (St)

|                                             |                                             |
|---------------------------------------------|---------------------------------------------|
| EI -- encapsulation invalid<br>CCC/TCC/VPLS | NC -- interface encapsulation not           |
| EM -- encapsulation mismatch<br>same        | WE -- interface and instance encaps not     |
| VC-Dn -- Virtual circuit down               | NP -- interface hardware not present        |
| CM -- control-word mismatch                 | -> -- only outbound connection is up        |
| CN -- circuit not provisioned               | <- -- only inbound connection is up         |
| OR -- out of range                          | Up -- operational                           |
| OL -- no outgoing label                     | Dn -- down                                  |
| LD -- local site signaled down              | CF -- call admission control failure        |
| RD -- remote site signaled down             | SC -- local and remote site ID collision    |
| LN -- local site not designated             | LM -- local site ID not minimum designated  |
| RN -- remote site not designated            | RM -- remote site ID not minimum designated |
| XX -- unknown connection status             | IL -- no incoming label                     |
| MM -- MTU mismatch                          | MI -- Mesh-Group ID not available           |
| BK -- Backup connection                     | ST -- Standby connection                    |

Legend for interface status

Up -- operational  
Dn -- down

Instance: GOLD

Local site: CE1 (1)

| connection-site | Type | St | Time last up        | # Up trans |
|-----------------|------|----|---------------------|------------|
| 3               | rmt  | Up | Oct 6 16:27:23 2009 | 1          |

Remote PE: 192.0.2.2, Negotiated control-word: No  
Incoming label: 262171, Outgoing label: 262145

```

Local interface: lsi.1049353, Status: Up, Encapsulation: VPLS
Description: Intf - vpls GOLD local site 1 remote site 3
4 rmt RM
5 rmt Up Oct 6 16:27:27 2009 1
Remote PE: 192.0.2.3, Negotiated control-word: No
Incoming label: 262173, Outgoing label: 262145
Local interface: lsi.1049354, Status: Up, Encapsulation: VPLS
Description: Intf - vpls GOLD local site 1 remote site 5
6 rmt Up Oct 6 16:27:31 2009 1
Remote PE: 192.0.2.4, Negotiated control-word: No
Incoming label: 262174, Outgoing label: 800000
Local interface: lsi.1049355, Status: Up, Encapsulation: VPLS
Description: Intf - vpls GOLD local site 1 remote site 6
Local site: Direct (2)
connection-site Type St Time last up # Up trans
3 rmt LM
4 rmt LM
5 rmt LM
6 rmt LM

```

- On Router PE4, use the **show vpls connections** command to verify the VPLS connections state.

Verify that site 2 and site 4 are in the **RM** state. This state tells you that the sites are configured with the highest site ID on Router PE1 and Router PE2. Because Router PE4 has only one site configured, it does not have any sites in the **LM** states.

```

user@PE4> show vpls connections
...
Instance: GOLD
Local site: Direct (6)
connection-site Type St Time last up # Up trans
1 rmt Up Oct 6 16:28:35 2009 1
Remote PE: 192.0.2.1, Negotiated control-word: No
Incoming label: 800000, Outgoing label: 262174
Local interface: vt-1/2/10.1048576, Status: Up, Encapsulation: VPLS
Description: Intf - vpls GOLD local site 6 remote site 1
2 rmt RM
3 rmt Up Oct 6 16:28:35 2009 1
Remote PE: 192.0.2.2, Negotiated control-word: No
Incoming label: 800002, Outgoing label: 262150
Local interface: vt-1/2/10.1048577, Status: Up, Encapsulation: VPLS
Description: Intf - vpls GOLD local site 6 remote site 3
4 rmt RM
5 rmt Up Oct 6 16:28:35 2009 1
Remote PE: 192.0.2.3, Negotiated control-word: No
Incoming label: 800004, Outgoing label: 262150
Local interface: vt-1/2/10.1048578, Status: Up, Encapsulation: VPLS
Description: Intf - vpls GOLD local site 6 remote site 5

```

- On each PE router, use the **show bgp summary** command to verify that the IBGP sessions between the PE routers or between the PE router and the route reflector have been established. The sessions must be operational before the PE routers can exchange any Layer 2 VPN routes. In the example below, also notice that the output from Router PE1 shows that the **bgp.l2vpn.0** and **GOLD.l2vpn.0** routing tables have been created.

```

user@PE1> show bgp summary
Groups: 1 Peers: 1 Down peers: 0
Table Tot Paths Act Paths Suppressed History Damp State Pending

```

```

bgp.12vpn.0 4 4 0 0 0 0
Peer AS InPkt OutPkt OutQ Flaps Last Up/Dwn State
192.0.2.7 65000 40 39 0 1 15:45 Establ

```

```

bgp.12vpn.0: 4/4/4/0
GOLD.12vpn.0: 4/4/4/0

```

```

admin@PE2# run show bgp summary
Groups: 1 Peers: 1 Down peers: 0
Table Tot Paths Act Paths Suppressed History Damp State Pending
bgp.12vpn.0 4 4 0 0 0 0 0
inet6.0 0 0 0 0 0 0 0
inet.0 0 0 0 0 0 0 0
Peer AS InPkt OutPkt OutQ Flaps Last Up/Dwn State
192.0.2.7 65000 43 42 0 0 17:25 Establ

```

```

bgp.12vpn.0: 4/4/4/0
GOLD.12vpn.0: 4/4/4/0

```

4. On Router PE4, use the **show route table** command to verify that there is one Layer 2 VPN route to each of the other PE routers. Router PE3 should have a similar **show** command output.

```

user@PE4> show route table bgp.12vpn.0
bgp.12vpn.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.1:1:1/96
 *[BGP/170] 00:23:18, localpref 100, from 192.0.2.7
 AS path: I
 > to 10.10.9.1 via xe-0/0/0.0, label-switched-path to-PE1
192.0.2.1:1:2:1/96
 *[BGP/170] 00:23:18, localpref 100, from 192.0.2.7
 AS path: I
 > to 10.10.9.1 via xe-0/0/0.0, label-switched-path to-PE1
192.0.2.2:10:3:1/96
 *[BGP/170] 00:23:18, localpref 100, from 192.0.2.7
 AS path: I
 > to 10.10.9.1 via xe-0/0/0.0, label-switched-path to-PE2
192.0.2.2:10:4:1/96
 *[BGP/170] 00:23:18, localpref 100, from 192.0.2.7
 AS path: I
 > to 10.10.9.1 via xe-0/0/0.0, label-switched-path to-PE2
192.0.2.3:10:5:1/96
 *[BGP/170] 00:23:18, localpref 100, from 192.0.2.7
 AS path: I
 > to 10.10.8.1 via xe-0/1/0.0, label-switched-path to-PE3

```

5. On the route reflector, use the **show bgp summary** command to verify that the router has an IBGP peer session with each of the PE routers.

```

user@RR> show bgp summary
Groups: 2 Peers: 5 Down peers: 1
Table Tot Paths Act Paths Suppressed History Damp State Pending
bgp.12vpn.0 6 6 0 0 0 0
inet.0 0 0 0 0 0 0
Peer AS InPkt OutPkt OutQ Flaps Last Up/Dwn State
192.0.2.1 65000 44 46 0 0 18:27 Establ

bgp.12vpn.0: 2/2/2/0
192.0.2.2 65000 43 45 0 0 18:22 Establ

```

```

 bgp.12vpn.0: 2/2/2/0
192.0.2.3 65000 42 45 0 0 18:19 Establ

```

```

 bgp.12vpn.0: 1/1/1/0
192.0.2.4 65000 43 45 0 0 18:15 Establ

```

```

 bgp.12vpn.0: 1/1/1/0

```

6. In NG-VPLS, point-to-multipoint LSPs carry only unknown unicast, broadcast, and multicast packets. A full mesh of point-to-point LSPs is needed between the PE routers for NG-VPLS. The point-to-point LSPs create routes in the **inet.3** routing table. These entries are used to resolve the Layer 2 VPN routes received from the BGP peers. All other data traffic is sent over point-to-point LSPs.

A point-to-point LSP is also created for the route reflector. This LSP creates a route in the **inet.3** routing table for BGP next-hop resolution.

On Router PE1, use the **show mpls lsp** command to verify that the **to-PE2**, **to-PE3**, **to-PE4**, and **to-RR** LSPs are in the **Up** state.

```

user@PE1> show mpls lsp ingress unidirectional

```

```

Ingress LSP: 7 sessions

```

| To        | From      | State | Rt | P | ActivePath | LSPName |
|-----------|-----------|-------|----|---|------------|---------|
| 192.0.2.2 | 192.0.2.1 | Up    | 0  | * |            | to-PE2  |
| 192.0.2.3 | 192.0.2.1 | Up    | 0  | * |            | to-PE3  |
| 192.0.2.4 | 192.0.2.1 | Up    | 0  | * |            | to-PE4  |
| 192.0.2.7 | 192.0.2.1 | Up    | 0  | * |            | to-RR   |

```

Total 4 displayed, Up 4, Down 0

```

```

admin@PE2# run show mpls lsp ingress unidirectional

```

```

Ingress LSP: 7 sessions

```

| To        | From      | State | Rt | P | ActivePath | LSPName |
|-----------|-----------|-------|----|---|------------|---------|
| 192.0.2.1 | 192.0.2.2 | Up    | 0  | * |            | to-PE1  |
| 192.0.2.3 | 192.0.2.2 | Up    | 0  | * |            | to-PE3  |
| 192.0.2.4 | 192.0.2.2 | Up    | 0  | * |            | to-PE4  |
| 192.0.2.7 | 192.0.2.2 | Up    | 0  | * |            | to-RR   |

```

Total 4 displayed, Up 4, Down 0

```

```

admin@PE3# run show mpls lsp ingress unidirectional

```

```

Ingress LSP: 7 sessions

```

| To        | From      | State | Rt | P | ActivePath | LSPName |
|-----------|-----------|-------|----|---|------------|---------|
| 192.0.2.1 | 192.0.2.3 | Up    | 0  | * |            | to-PE1  |
| 192.0.2.2 | 192.0.2.3 | Up    | 0  | * |            | to-PE2  |
| 192.0.2.4 | 192.0.2.3 | Up    | 0  | * |            | to-PE4  |
| 192.0.2.7 | 192.0.2.3 | Up    | 0  | * |            | to-RR   |

```

Total 4 displayed, Up 4, Down 0

```

```

admin@PE4# run show mpls lsp ingress unidirectional

```

```

Ingress LSP: 7 sessions

```

| To        | From      | State | Rt | P | ActivePath | LSPName |
|-----------|-----------|-------|----|---|------------|---------|
| 192.0.2.1 | 192.0.2.4 | Up    | 0  | * |            | to-PE1  |
| 192.0.2.2 | 192.0.2.4 | Up    | 0  | * |            | to-PE2  |
| 192.0.2.3 | 192.0.2.4 | Up    | 0  | * |            | to-PE3  |
| 192.0.2.7 | 192.0.2.4 | Up    | 0  | * |            | to-RR   |

```

Total 4 displayed, Up 4, Down 0

```

7. For each VPLS instance, a PE router creates a dedicated point-to-multipoint LSP. In this example, Router PE1 and Router PE2 are configured to use a point-to-multipoint dynamic template.

For dynamic point-to-multipoint LSPs, whenever VPLS discovers a new Layer 2 VPN neighbor through BGP, a source-to-leaf sub-LSP is added in the VPLS instance for this neighbor PE router.

On Router PE1, use the **show mpls lsp** command to verify that three source-to-leaf sub-LSPs are created.

```
user@PE1> show mpls lsp ingress p2mp
Ingress LSP: 1 sessions
P2MP name: 192.0.2.1:1:vp1s:GOLD, P2MP branch count: 3
To From State Rt P ActivePath LSPname
192.0.2.4 192.0.2.1 Up 0 *
192.0.2.4:192.0.2.1:1:vp1s:GOLD
192.0.2.3 192.0.2.1 Up 0 *
192.0.2.3:192.0.2.1:1:vp1s:GOLD
192.0.2.2 192.0.2.1 Up 0 *
192.0.2.2:192.0.2.1:1:vp1s:GOLD
Total 3 displayed, Up 3, Down 0
```

8. On Router PE2, use the **show mpls lsp** command to verify that three source-to-leaf sub-LSPs are created.

```
user@PE2> show mpls lsp p2mp ingress
Ingress LSP: 1 sessions
P2MP name: 192.0.2.2:10:vp1s:GOLD, P2MP branch count: 3
To From State Rt P ActivePath LSPname
192.0.2.4 192.0.2.2 Up 0 *
192.0.2.4:192.0.2.2:10:vp1s:GOLD
192.0.2.3 192.0.2.2 Up 0 *
192.0.2.3:192.0.2.2:10:vp1s:GOLD
192.0.2.1 192.0.2.2 Up 0 *
192.0.2.1:192.0.2.2:10:vp1s:GOLD
Total 3 displayed, Up 3, Down 0
```

9. In this step, Router PE3 and Router PE4 are using static point-to-multipoint LSPs. For static point-to-multipoint LSPs, the source-to-leaf sub-LSPs to all the PE routers are manually configured.

On Router PE3, use the **show mpls lsp** command to verify that three source-to-leaf sub-LSPs have been configured.

```
user@PE3> show mpls lsp p2mp ingress
Ingress LSP: 1 sessions
P2MP name: vp1s-GOLD, P2MP branch count: 3
To From State Rt P ActivePath LSPname
192.0.2.1 192.0.2.3 Up 0 * to-pe1
192.0.2.4 192.0.2.3 Up 0 * to-pe4
192.0.2.2 192.0.2.3 Up 0 * to-pe2
Total 3 displayed, Up 3, Down 0
```

10. On Router PE4, use the **show mpls lsp** command to verify that three source-to-leaf sub-LSPs are configured.

```
user@PE4> show mpls lsp ingress p2mp
Ingress LSP: 1 sessions
P2MP name: vp1s-GOLD, P2MP branch count: 3
To From State Rt P ActivePath LSPname
192.0.2.1 192.0.2.4 Up 0 * to-pe1
192.0.2.3 192.0.2.4 Up 0 * to-pe3
192.0.2.2 192.0.2.4 Up 0 * to-pe2
Total 3 displayed, Up 3, Down 0
```

11. Each point-to-multipoint LSP created by the PE router can be identified using an RSVP-TE point-to-multipoint session object. The session object is passed as a PMSI tunnel attribute by BGP when it advertises VPLS routes. Using this tunnel attribute, an incoming source-to-leaf sub LSP add request (RSVP-Path message) supports label allocation in such a way that when traffic arrives on this source-to-leaf sub-LSP the router terminates the message in the right VPLS instance and also identifies the originating PE. This supports source MAC address learning.

On Router PE1, use the **show rsvp session** command to verify that the RSVP session for the dynamic point-to-multipoint LSP is **Up** and that link protection is configured as **desired**. Notice that the point-to-multipoint session object to be sent in BGP is **54337**.

```
user@PE1> show rsvp session detail p2mp ingress
Ingress RSVP: 7 sessions
P2MP name: 192.0.2.1:1:vp1s:GOLD, P2MP branch count: 3

192.0.2.2
 From: 192.0.2.1, LSPstate: Up, ActiveRoute: 0
 LSPname: 192.0.2.2:192.0.2.1:1:vp1s:GOLD, LSPpath: Primary
 P2MP LSPname: 192.0.2.1:1:vp1s:GOLD
 Suggested label received: -, Suggested label sent: -
 Recovery label received: -, Recovery label sent: 262145
 Resv style: 1 SE, Label in: -, Label out: 262145
 Time left: -, Since: Tue Oct 6 16:27:23 2009
 Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
 Port number: sender 2 receiver 54337 protocol 0
 Link protection desired
 Type: Protection down
 PATH rcvfrom: localclient
 Adspec: sent MTU 1500
 Path MTU: received 1500
 PATH sentto: 10.10.2.2 (xe-0/1/0.0) 371 pkts
 RESV rcvfrom: 10.10.2.2 (xe-0/1/0.0) 370 pkts
 Explct route: 10.10.2.2
 Record route: <self> 10.10.2.2
```

12. Router PE4 is configured for static point-to-multipoint LSPs. Link protection is not configured for these LSPs. Use the **show rsvp session** command to verify that the point-to-multipoint session object to be sent in BGP is **42873**.

```
user@PE4> show rsvp session detail p2mp ingress
Ingress RSVP: 7 sessions
P2MP name: vp1s-GOLD, P2MP branch count: 3

192.0.2.1
 From: 192.0.2.4, LSPstate: Up, ActiveRoute: 0
 LSPname: to-pe1, LSPpath: Primary
 P2MP LSPname: vp1s-GOLD
 Suggested label received: -, Suggested label sent: -
 Recovery label received: -, Recovery label sent: 390416
 Resv style: 1 SE, Label in: -, Label out: 390416
 Time left: -, Since: Tue Oct 6 15:28:33 2009
 Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
 Port number: sender 10 receiver 42873 protocol 0
 PATH rcvfrom: localclient
 Adspec: sent MTU 1500
 Path MTU: received 1500
 PATH sentto: 10.10.9.1 (xe-0/0/0.0) 524 pkts
```

```

RESV rcvfrom: 10.10.9.1 (xe-0/0/0.0) 447 pkts
Explot route: 10.10.9.1 10.10.3.1
Record route: <self> 10.10.9.1 10.10.3.1

```

13. On Router PE1, use the **show route table** command to verify that Router PE1 received a Layer 2 VPN route to Router PE2 from the router reflector and the route includes a PMSI object that contains the point-to-multipoint tunnel identifier of **20361**.

```

user@PE1> show route table GOLD.l2vpn.0 detail
GOLD.l2vpn.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
!
!
192.0.2.2:10:3:1/96 (1 entry, 1 announced)
 *BGP Preference: 170/-101
 Route Distinguisher: 192.0.2.2:10
 PMSI: Flags 0:RSVP-TE:label[0:0:0]:Session_13[192.0.2.2:0:20361:192.0.2.2]
 Next hop type: Indirect
 Next-hop reference count: 7
 Source: 192.0.2.7
 Protocol next hop: 192.0.2.2
 Indirect next hop: 2 no-forward
 State: <Secondary Active Int Ext>
 Local AS: 65000 Peer AS: 65000
 Age: 4:25:25 Metric2: 1
 Task: BGP_65000.192.0.2.7+63544
 Announcement bits (1): 0-GOLD-l2vpn
 AS path: I (Originator) Cluster list: 192.0.2.7
 AS path: Originator ID: 192.0.2.2
 Communities: target:65000:1 Layer2-info: encaps:VPLS, control flags:, mtu: 0, site
preference: 100
 Import Accepted
 Label-base: 262145, range: 8
 Localpref: 100
 Router ID: 192.0.2.7
 Primary Routing Table bgp.l2vpn.0
PMSI: Flags 0:RSVP-TE:label[0:0:0]:Session_13[192.0.2.2:0:20361:192.0.2.2]

```

14. On Router PE2, use the **show rsvp session** command to verify that the PMSI tunnel identifier object of **20361** matches the PMSI tunnel identifier object displayed on Router PE1.

```

user@PE2> show rsvp session p2mp detail
Ingress RSVP: 7 sessions
P2MP name: 192.0.2.2:10:vp1s:GOLD, P2MP branch count: 3

192.0.2.1
 From: 192.0.2.2, LSPstate: Up, ActiveRoute: 0
 LSPname: 192.0.2.1:192.0.2.2:10:vp1s:GOLD, LSPpath: Primary
 P2MP LSPname: 192.0.2.2:10:vp1s:GOLD
 Suggested label received: -, Suggested label sent: -
 Recovery label received: -, Recovery label sent: 262171
 Resv style: 1 SE, Label in: -, Label out: 262171
 Time left: -, Since: Tue Oct 6 16:31:47 2009
 Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
 Port number: sender 1 receiver 20361 protocol 0
 Link protection desired
 Type: Protection down
 PATH rcvfrom: localclient
 Adspec: sent MTU 1500
 Path MTU: received 1500
 PATH sentto: 10.10.2.1 (xe-0/1/0.0) 379 pkts

```



```

RESV rcvfrom: 10.10.2.1 (xe-0/1/0.0) 379 pkts
Exp1ct route: 10.10.2.1
Record route: <self> 10.10.2.1

```

### Verifying the Data Plane

**Step-by-Step Procedure** After the control plane is verified using the previous steps, you can verify the data plane. This section describes **show** command outputs you can use to validate the data plane.

1. On Router PE1, use the **show vpls connections extensive | match Flood** command to verify the point-to-multipoint LSP name and status of all the sites. Notice the flood next-hop identifier of **600** for the **192.0.2.1:1:vpls:GOLD** LSP.

```

user@PE1> show vpls connections extensive | match Flood
Ingress RSVP-TE P2MP LSP: 192.0.2.1:1:vpls:GOLD, Flood next-hop ID: 600

```

2. On Router PE1, use the **show vpls connections extensive** command to verify the point-to-multipoint LSP name and status of all the sites.

```

user@PE1> show vpls connections extensive
Instance: GOLD
Local site: CE1 (1)
 Number of local interfaces: 1
 Number of local interfaces up: 1
 IRB interface present: no
 ge-1/0/0.1
 lsi.1049353 3 Intf - vpls GOLD local site 1 remote site 3
 lsi.1049346 4 Intf - vpls GOLD local site 1 remote site 4
 Interface flags: VC-Down
 lsi.1049354 5 Intf - vpls GOLD local site 1 remote site 5
 lsi.1049355 6 Intf - vpls GOLD local site 1 remote site 6
Label-base Offset Range Preference
262169 1 8 100
connection-site Type St Time last up # Up trans
3 rmt Up Oct 6 16:27:23 2009 1
 Remote PE: 192.0.2.2, Negotiated control-word: No
 Incoming label: 262171, Outgoing label: 262145
 Local interface: lsi.1049353, Status: Up, Encapsulation: VPLS
 Description: Intf - vpls GOLD local site 1 remote site 3
 RSVP-TE P2MP lsp:
 Ingress branch LSP: 192.0.2.2:192.0.2.1:1:vpls:GOLD, State: Up
 Egress branch LSP: 192.0.2.1:192.0.2.2:10:vpls:GOLD, State: Up
Connection History:
 Oct 6 16:27:23 2009 status update timer
 Oct 6 16:27:23 2009 PE route changed
 Oct 6 16:27:23 2009 Out lbl Update 262145
 Oct 6 16:27:23 2009 In lbl Update 262171
 Oct 6 16:27:23 2009 loc intf up lsi.1049353
4 rmt RM
 RSVP-TE P2MP lsp:
 Ingress branch LSP: 192.0.2.2:192.0.2.1:1:vpls:GOLD, State: Up
5 rmt Up Oct 6 16:27:27 2009 1
 Remote PE: 192.0.2.3, Negotiated control-word: No
 Incoming label: 262173, Outgoing label: 262145
 Local interface: lsi.1049354, Status: Up, Encapsulation: VPLS
 Description: Intf - vpls GOLD local site 1 remote site 5
 RSVP-TE P2MP lsp:
 Ingress branch LSP: 192.0.2.3:192.0.2.1:1:vpls:GOLD, State: Up
 Egress branch LSP: to-pe1, State: Up
Connection History:

```

```

Oct 6 16:27:27 2009 status update timer
Oct 6 16:27:27 2009 PE route changed
Oct 6 16:27:27 2009 Out lbl Update 262145
Oct 6 16:27:27 2009 In lbl Update 262173
Oct 6 16:27:27 2009 loc intf up lsi.1049354
6 rmt Up Oct 6 16:27:31 2009 1
Remote PE: 192.0.2.4, Negotiated control-word: No
Incoming label: 262174, Outgoing label: 800000
Local interface: lsi.1049355, Status: Up, Encapsulation: VPLS
Description: Intf - vpls GOLD local site 1 remote site 6
RSVP-TE P2MP lsp:
Ingress branch LSP: 192.0.2.4:192.0.2.1:1:vpls:GOLD, State: Up
Egress branch LSP: to-pe1, State: Up
Connection History:
Oct 6 16:27:31 2009 status update timer
Oct 6 16:27:31 2009 PE route changed
Oct 6 16:27:31 2009 Out lbl Update 800000
Oct 6 16:27:31 2009 In lbl Update 262174
Oct 6 16:27:31 2009 loc intf up lsi.1049355
Local site: Direct (2)
Number of local interfaces: 1
Number of local interfaces up: 1
IRB interface present: no
Interface name Remote site ID Description
ge-1/1/0.1
lsi.1049347 3 Intf - vpls GOLD local site 2 remote site 3
Interface flags: VC-Down
lsi.1049348 4 Intf - vpls GOLD local site 2 remote site 4
Interface flags: VC-Down
lsi.1049350 5 Intf - vpls GOLD local site 2 remote site 5
Interface flags: VC-Down
lsi.1049352 6 Intf - vpls GOLD local site 2 remote site 6
Interface flags: VC-Down
Label-base Offset Range Preference
262177 1 8 100
connection-site Type St Time last up
3 rmt LM
RSVP-TE P2MP lsp:
Ingress branch LSP: 192.0.2.2:192.0.2.1:1:vpls:GOLD, State: Up
4 rmt LM
RSVP-TE P2MP lsp:
Ingress branch LSP: 192.0.2.2:192.0.2.1:1:vpls:GOLD, State: Up
5 rmt LM
RSVP-TE P2MP lsp:
Ingress branch LSP: 192.0.2.3:192.0.2.1:1:vpls:GOLD, State: Up
6 rmt LM
RSVP-TE P2MP lsp:
Ingress branch LSP: 192.0.2.4:192.0.2.1:1:vpls:GOLD, State: Up
Ingress RSVP-TE P2MP LSP: 192.0.2.1:1:vpls:GOLD, Flood next-hop ID: 600

```

3. Junos OS Release 9.0 and later identifies the flood next-hop route as a composite next hop. On Router PE1, use the **show route forwarding-table family vpls vpn GOLD detail** command to verify that three composite flood next-hop routes are installed in the Packet Forwarding Engine.

```
user@PE1> show route forwarding-table family vpls vpn GOLD detail
```

```
Routing table: GOLD.vpls
```

```
VPLS:
```

| Destination | Type | RtRef | Next hop | Type | Index | NhRef | Netif |
|-------------|------|-------|----------|------|-------|-------|-------|
| default     | perm | 0     |          | dscd | 518   | 1     |       |

```
00:00:28:28:28:02/48
```

```

00:00:28:28:28:06/48 user 0 ucst 617 4 ge-1/1/0.1
00:00:28:28:28:06/48 user 0 indr 1048576 4
1si.1049353 intf 0 Push 800000, Push 390384(top) 621 2 xe-0/2/0.0
1si.1049353 intf 0 indr 1048574 3
1si.1049354 intf 0 Push 262145 598 2 xe-0/1/0.0
1si.1049354 intf 0 indr 1048575 4
1si.1049355 intf 0 Push 262145, Push 302272(top) 602 2 xe-0/3/0.0
1si.1049355 intf 0 indr 1048576 4
00:14:f6:75:78:00/48 user 0 Push 800000, Push 390384(top) 621 2 xe-0/2/0.0
00:14:f6:75:78:00/48 user 0 indr 1048575 4
00:19:e2:57:e7:c0/48 user 0 Push 262145, Push 302272(top) 602 2 xe-0/3/0.0
00:19:e2:57:e7:c0/48 user 0 indr 1048575 4
0x30003/51 user 0 ucst 604 4 ge-1/0/0.1
0x30002/51 user 0 comp 613 2
0x30001/51 user 0 comp 615 2
0x30001/51 user 0 comp 582 2
ge-1/0/0.1 intf 0 ucst 604 4 ge-1/0/0.1
ge-1/1/0.1 intf 0 ucst 617 4 ge-1/1/0.1

```

You can also use the **show route forwarding-table family vpls extensive** command to match the flood identifier and note the flood label. To match the label out corresponding to the point-to-multipoint LSP, use the **show rsvp session ingress p2mp** command.

- On Router PE1, use the **show route forwarding-table family vpls vpn GOLD extensive | find 0x30003/51** command to get more details about the composite next-hop route and the associated point-to-multipoint LSP labels.

```

user@PE1> show route forwarding-table family vpls vpn GOLD extensive | find 0x30003/51
Destination: 0x30003/51

```

```

Route type: user
Route reference: 0
Flags: sent to PFE
Nexthop:
Next-hop type: composite Index: 613 Reference: 2
Nexthop:
Next-hop type: composite Index: 556 Reference: 4
Next-hop type: unicast Index: 604 Reference: 4
Next-hop interface: ge-1/0/0.1
Next-hop type: unicast Index: 617 Reference: 4
Next-hop interface: ge-1/1/0.1

```

```

Destination: 0x30002/51
Route type: user
Route reference: 0
Flags: sent to PFE
Nexthop:
Next-hop type: composite Index: 615 Reference: 2
Nexthop:
Next-hop type: composite Index: 556 Reference: 4
Next-hop type: unicast Index: 604 Reference: 4
Next-hop interface: ge-1/0/0.1
Next-hop type: unicast Index: 617 Reference: 4
Next-hop interface: ge-1/1/0.1
Nexthop:
Next-hop type: composite Index: 603 Reference: 3
Next-hop type: flood Index: 600 Reference: 2
Nexthop: 10.10.2.2

```

|                                |            |              |
|--------------------------------|------------|--------------|
| Next-hop type: Push 262145     | Index: 599 | Reference: 1 |
| Next-hop interface: xe-0/1/0.0 |            |              |
| Nexthop: 10.10.3.2             |            |              |
| Next-hop type: Push 390496     | Index: 622 | Reference: 1 |
| Next-hop interface: xe-0/2/0.0 |            |              |
| Nexthop: 10.10.1.2             |            |              |
| Next-hop type: Push 302416     | Index: 618 | Reference: 1 |
| Next-hop interface: xe-0/3/0.0 |            |              |

Destination: 0x30001/51  
Route type: user  
Route reference: 0  
Flags: sent to PFE  
Nexthop:  
Route interface-index: 0

|                                |            |              |
|--------------------------------|------------|--------------|
| Next-hop type: composite       | Index: 582 | Reference: 2 |
| Nexthop:                       |            |              |
| Next-hop type: composite       | Index: 556 | Reference: 4 |
| Next-hop type: unicast         | Index: 604 | Reference: 4 |
| Next-hop interface: ge-1/0/0.1 |            |              |
| Next-hop type: unicast         | Index: 617 | Reference: 4 |
| Next-hop interface: ge-1/1/0.1 |            |              |
| Nexthop:                       |            |              |
| Next-hop type: composite       | Index: 603 | Reference: 3 |
| Next-hop type: flood           | Index: 600 | Reference: 2 |
| Nexthop: 10.10.2.2             |            |              |
| Next-hop type: Push 262145     | Index: 599 | Reference: 1 |
| Next-hop interface: xe-0/1/0.0 |            |              |
| Nexthop: 10.10.3.2             |            |              |
| Next-hop type: Push 390496     | Index: 622 | Reference: 1 |
| Next-hop interface: xe-0/2/0.0 |            |              |
| Nexthop: 10.10.1.2             |            |              |
| Next-hop type: Push 302416     | Index: 618 | Reference: 1 |
| Next-hop interface: xe-0/3/0.0 |            |              |

Destination: ge-1/0/0.1  
Route type: interface  
Route reference: 0  
Flags: sent to PFE  
Next-hop type: unicast  
Next-hop interface: ge-1/0/0.1  
Route interface-index: 84  
Index: 604 Reference: 4

Destination: ge-1/1/0.1  
Route type: interface  
Route reference: 0  
Flags: sent to PFE  
Next-hop type: unicast  
Next-hop interface: ge-1/1/0.1  
Route interface-index: 86  
Index: 617 Reference: 4

5. On Router PE1, use the **show vpls mac-table instance GOLD** command to verify the learned MAC addresses of CE routers connected to the VPLS domain.

```
user@PE1> show vpls mac-table instance GOLD
MAC flags (S -static MAC, D -dynamic MAC,
SE -Statistics enabled, NM -Non configured MAC)
```

```
Routing instance : GOLD
Bridging domain : __GOLD__, VLAN : NA
MAC MAC Logical
address flags interface
00:00:28:28:28:02 D ge-1/1/0.1
00:00:28:28:28:04 D lsi.1049353
```

```

00:14:f6:75:78:00 D lsi.1049354
00:19:e2:51:7f:c0 D lsi.1049353
00:19:e2:57:e7:c0 D ge-1/0/0.1

```

6. On Router PE1, use the **show vpls statistics** command to verify the broadcast, multicast, and unicast traffic flow using the packet statistics for the VPLS instance.

```
user@PE1> show vpls statistics
```

```
VPLS statistics:
```

```

Instance: GOLD
 Local interface: lsi.1049347, Index: 72
 Current MAC count: 0
 Local interface: lsi.1049348, Index: 73
 Current MAC count: 0
 Local interface: lsi.1049346, Index: 82
 Current MAC count: 0
 Local interface: lsi.1049353, Index: 83
 Remote PE: 192.0.2.2
 Current MAC count: 2
 Local interface: ge-1/0/0.1, Index: 84
 Broadcast packets: 421
 Broadcast bytes : 26944
 Multicast packets: 3520
 Multicast bytes : 261906
 Flooded packets : 509043345
 Flooded bytes : 130315095486
 Unicast packets : 393836428
 Unicast bytes : 100822118854
 Current MAC count: 1 (Limit 1024)
 Local interface: ge-1/1/0.1, Index: 86
 Broadcast packets: 0
 Broadcast bytes : 0
 Multicast packets: 0
 Multicast bytes : 0
 Flooded packets : 22889544
 Flooded bytes : 5859702144
 Unicast packets : 472
 Unicast bytes : 30838
 Current MAC count: 1 (Limit 1024)
 Local interface: lsi.1049354, Index: 88
 Remote PE: 192.0.2.3
 Current MAC count: 1
 Local interface: lsi.1049350, Index: 89
 Current MAC count: 0
 Local interface: lsi.1049355, Index: 90
 Remote PE: 192.0.2.4
 Current MAC count: 0
 Local interface: lsi.1049352, Index: 91
 Current MAC count: 0

```

## Results

The configuration, verification, and testing part of this example has been completed. The following section is for your reference.

The relevant sample configuration for Router PE1 follows.

```

PE1 Configuration chassis {
 dump-on-panic;

```

```
fpc 1 {
 pic 3 {
 tunnel-services {
 bandwidth 1g;
 }
 }
}
network-services ethernet;
}
interfaces {
 xe-0/1/0 {
 unit 0 {
 family inet {
 address 10.10.2.1/30;
 }
 family mpls;
 }
 }
 xe-0/2/0 {
 unit 0 {
 family inet {
 address 10.10.3.1/30;
 }
 family mpls;
 }
 }
 xe-0/3/0 {
 unit 0 {
 family inet {
 address 10.10.1.1/30;
 }
 family mpls;
 }
 }
 ge-1/0/0 {
 vlan-tagging;
 encapsulation vlan-vpls;
 unit 1 {
 encapsulation vlan-vpls;
 vlan-id 1000;
 family vpls;
 }
 }
 ge-1/1/0 {
 vlan-tagging;
 encapsulation vlan-vpls;
 unit 1 {
 encapsulation vlan-vpls;
 vlan-id 1000;
 family vpls;
 }
 }
 lo0 {
 unit 0 {
 family inet {
 address 192.0.2.1/24;
 }
 }
 }
}
```

```

 }
 }
}
routing-options {
 static {
 route 172.16.0.0/8 next-hop 172.19.59.1;
 }
 autonomous-system 65000;
}
protocols {
 rsvp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 mpls {
 label-switched-path to-RR {
 to 192.0.2.7;
 }
 label-switched-path vpls-GOLD-p2mp-template {
 template;
 optimize-timer 50;
 link-protection;
 p2mp;
 }
 label-switched-path to-PE2 {
 to 192.0.2.2;
 }
 label-switched-path to-PE3 {
 to 192.0.2.3;
 }
 label-switched-path to-PE4 {
 to 192.0.2.4;
 }
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 bgp {
 group to-RR {
 type internal;
 local-address 192.0.2.1;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {

```

```

 disable;
 }
}
}
routing-instances {
 GOLD {
 instance-type vpls;
 interface ge-1/0/0.1;
 interface ge-1/1/0.1;
 route-distinguisher 192.0.2.1:1;
 provider-tunnel {
 rsvp-te {
 label-switched-path-template {
 vpls-GOLD-p2mp-template;
 }
 }
 }
 vrf-target target:65000:1;
 protocols {
 vpls {
 site-range 8;
 no-tunnel-services;
 site CE1 {
 site-identifier 1;
 interface ge-1/0/0.1;
 }
 site Direct {
 site-identifier 2;
 interface ge-1/1/0.1;
 }
 }
 }
 }
}
}

```

The relevant sample configuration for Router PE2 follows.

|                          |                                                                                                                                                                                                                                                                              |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PE2 Configuration</b> | <pre> chassis {     dump-on-panic;     aggregated-devices {         ethernet {             device-count 1;         }     } } fpc 1 {     pic 3 {         tunnel-services {             bandwidth 1g;         }     } } } interfaces {     xe-0/1/0 {         unit 0 { </pre> |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



```
 family inet {
 address 10.10.2.2/30;
 }
 family mpls;
 }
}
xe-0/2/0 {
 unit 0 {
 family inet {
 address 10.10.5.1/30;
 }
 family mpls;
 }
}
xe-0/3/0 {
 unit 0 {
 family inet {
 address 10.10.4.1/30;
 }
 family mpls;
 }
}
ge-1/0/1 {
 gigether-options {
 802.3ad ae0;
 }
}
ge-1/0/2 {
 gigether-options {
 802.3ad ae0;
 }
}
ge-1/1/0 {
 vlan-tagging;
 encapsulation vlan-vpls;
 unit 1 {
 encapsulation vlan-vpls;
 vlan-id 1000;
 family vpls;
 }
}
ae0 {
 vlan-tagging;
 encapsulation vlan-vpls;
 unit 1 {
 encapsulation vlan-vpls;
 vlan-id 1000;
 family vpls;
 }
}
fxp0 {
 apply-groups [re0 re1];
}
lo0 {
 unit 0 {
 family inet {
```

```
 address 192.0.2.2/24;
 }
}
}
routing-options {
 static {
 route 172.16.0.0/8 next-hop 172.19.59.1;
 }
 autonomous-system 65000;
}
protocols {
 rsvp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 mpls {
 label-switched-path to-RR {
 to 192.0.2.7;
 }
 label-switched-path vpls-GOLD-p2mp-template {
 template;
 optimize-timer 50;
 link-protection;
 p2mp;
 }
 label-switched-path to-PE1 {
 to 192.0.2.1;
 }
 label-switched-path to-PE3 {
 to 192.0.2.3;
 }
 label-switched-path to-PE4 {
 to 192.0.2.4;
 }
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 bgp {
 group to-RR {
 type internal;
 local-address 192.0.2.2;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 }
 }
}
```

```

 interface fxp0.0 {
 disable;
 }
 }
}
routing-instances {
 GOLD {
 instance-type vpls;
 interface ge-1/1/0.1;
 interface ae0.1;
 route-distinguisher 192.0.2.2:10;
 provider-tunnel {
 rsvp-te {
 label-switched-path-template {
 vpls-GOLD-p2mp-template;
 }
 }
 }
 vrf-target target:65000:1;
 protocols {
 vpls {
 site-range 8;
 site CE1 {
 site-identifier 3;
 interface ae0.1;
 }
 site Direct {
 site-identifier 4;
 interface ge-1/1/0.1;
 }
 }
 }
 }
}
}

```

**Related Documentation** • [Next-Generation VPLS Point-to-Multipoint Forwarding Overview on page 809](#)

## Flooding Unknown Traffic Using Point-to-Multipoint LSPs in VPLS

For a VPLS routing instance, you can flood unknown unicast, broadcast, and multicast traffic using point-to-multipoint (also called *P2MP*) LSPs. By default, VPLS relies upon ingress replication to flood unknown traffic to the members of a VPLS routing instance. This can cause replication of data at routing nodes shared by multiple VPLS members, as shown in [Figure 76 on page 848](#). The flood data is tripled between PE router PE1 and provider router P1 and doubled between provider routers P1 and P2. By configuring point-to-multipoint LSPs to handle flood traffic, the VPLS routing instance can avoid this type of traffic replication in the network, as shown in [Figure 77 on page 848](#).

Figure 76: Flooding Unknown VPLS Traffic Using Ingress Replication

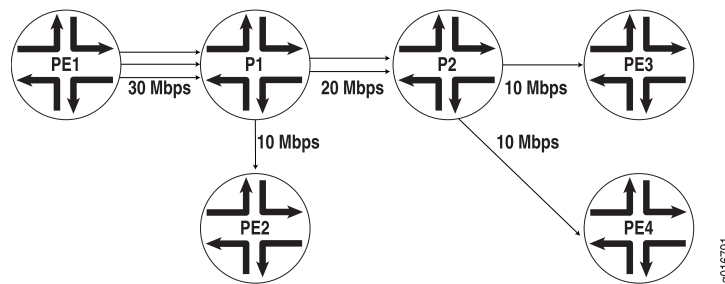
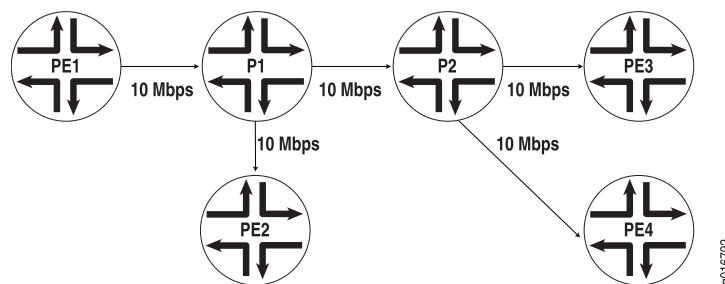


Figure 77: Flooding Unknown VPLS Traffic Using a Point-to-Multipoint LSP



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

The point-to-multipoint LSP used for VPLS flooding can be either static or dynamic. In either case, for each VPLS routing instance, the PE router creates a dedicated point-to-multipoint LSP. All of the neighbors of the VPLS routing instance are added to the point-to-multipoint LSP when the feature is enabled. If there are  $n$  PE routers in the VPLS routing instance,  $n$  point-to-multipoint LSPs are created in the network where each PE router is the root of the point-to-multipoint tree and includes the rest of the  $n - 1$  PE routers as leaf nodes. If you configured static point-to-multipoint LSPs for flooding, any additional VPLS neighbors added to the routing instance later are not automatically added to the point-to-multipoint LSP. You will need to manually add the new VPLS neighbors to the static point-to-multipoint flooding LSP. If you configure dynamic point-to-multipoint LSPs, whenever VPLS discovers a new neighbor through BGP, a sub-LSP for this neighbor is added to the point-to-multipoint LSP for the routing instance.

This feature can be enabled incrementally on any PE router that is part of a specific VPLS routing instance. The PE routers can then use point-to-multipoint LSPs to flood traffic, whereas other PE routers in the same VPLS routing instance can still use ingress replication to flood traffic. However, when this feature is enabled on any PE router, you must ensure that all PE routers in the VPLS routing instance that participate in the flooding of traffic over point-to-multipoint LSPs are upgraded to Junos OS Release 8.3 or later to support this feature.

To flood unknown unicast, broadcast, and multicast traffic using point-to-multipoint LSPs, configure the **rsvp-te** statement as follows:

```

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

```

You can include this statement at the following hierarchy levels:

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

You can configure either a static point-to-multipoint LSP for VPLS flooding or a dynamic point-to-multipoint LSP.



**NOTE:** You cannot specify both the static and label-switched-path-template statements at the same time.

The following sections describe how to configure static and dynamic point-to-multipoint LSPs for flooding unknown traffic in a VPLS routing instance:

- [Configuring Static Point-to-Multipoint Flooding LSPs on page 849](#)
- [Configuring Dynamic Point-to-Multipoint Flooding LSPs on page 850](#)

## Configuring Static Point-to-Multipoint Flooding LSPs

The **static-lsp** option creates a static flooding point-to-multipoint LSP that includes all of the neighbors in the VPLS routing instance. Flood traffic is sent to all of the VPLS neighbors using the generated point-to-multipoint LSP. VPLS neighbors added to the routing instance later are not automatically added to the point-to-multipoint LSP. You will need to manually add the new VPLS neighbors to the static point-to-multipoint flooding LSP. By configuring static point-to-multipoint LSPs for flooding, you have more control over which path each sub-LSP follows.

To configure a static flooding point-to-multipoint LSP, specify the name of the static flooding point-to-multipoint LSP by including 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]

## Configuring Dynamic Point-to-Multipoint Flooding LSPs

To configure a dynamic point-to-multipoint flooding LSP, include the **label-switched-path-template** statement option at the **[edit routing-instances routing-instance-name provider-tunnel rsvp-te]** hierarchy level:

```
[edit routing-instances routing-instance-name provider-tunnel rsvp-te]
label-switched-path-template (Multicast) {
 (default-template | lsp-template-name);
}
```

You can automatically generate the point-to-multipoint LSP to be used for flooding unknown traffic or you can manually configure the point-to-multipoint LSP:

- [Configuring Dynamic Point-to-Multipoint Flooding LSPs with the Default Template on page 850](#)
- [Configuring Dynamic Point-to-Multipoint Flooding LSPs with a Preconfigured Template on page 850](#)

### Configuring Dynamic Point-to-Multipoint Flooding LSPs with the Default Template

The **default-template** option, specified at the **[edit routing-instances routing-instance-name provider-tunnel rsvp-te label-switched-path-template]** hierarchy level, causes the point-to-multipoint LSPs to be created with default parameters. The default parameters are for a minimally configured point-to-multipoint LSP. The name of this point-to-multipoint LSP is also generated automatically and is based on the following model:

**id:vp1s:router-id:routing-instance-name**

The following **show** command output for **show mpls lsp p2mp** illustrates how a point-to-multipoint flood LSP name could appear if you configure the **label-switched-path-template** statement with the **default-template** option:

```
user@host> show mpls lsp p2mp ingress
Ingress LSP: 2 sessions P2MP name: static, P2MP branch count: 3
To From State Rt ActivePath P LSPname
10.255.14.181 10.255.14.172 Up 0 * * vpn02-vpn11
10.255.14.177 10.255.14.172 Up 0 path2 * vpn02-vpn07
10.255.14.174 10.255.14.172 Up 0 path3 * vpn02-vpn04
P2MP name: 9:vp1s:10.255.14.172:green, P2MP branch count: 2
To From State Rt ActivePath P LSPname
10.255.14.177 10.255.14.172 Up 0 * *
11:vp1s:10.255.14.172:green
10.255.14.174 10.255.14.172 Up 0 * *
10:vp1s:10.255.14.172:green
Total 5 displayed, Up 5, Down 0
```

The dynamically generated point-to-multipoint LSP name is **9:vp1s:10.255.14.172:green**.

### Configuring Dynamic Point-to-Multipoint Flooding LSPs with a Preconfigured Template

You can configure a point-to-multipoint flooding LSP template for the VPLS routing instance. The template allows you to specify the properties of the dynamic

point-to-multipoint LSPs that are used to flood traffic for the VPLS routing instance. You can specify all of the standard options available for a point-to-multipoint LSP within this template. These properties are inherited by the dynamic point-to-multipoint flood LSPs.

To configure a point-to-multipoint LSP template for flooding VPLS traffic, specify all of the properties you want to include in a point-to-multipoint LSP configuration. To specify this LSP as a point-to-multipoint flooding template, include the **p2mp** and **template** statements:

```
p2mp;
template;
```

You can include these statements at the following hierarchy levels:

- [edit protocols mpls label-switched-path *p2mp-lsp-template-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *p2mp-lsp-template-name*]

For more information about how to configure the **p2mp** statement and point-to-multipoint LSPs, see the *Junos OS MPLS Applications Library for Routing Devices*.

Once you have configured the point-to-multipoint LSP template, specify the name of the point-to-multipoint LSP template with the **label-switched-path-template** statement:

```
label-switched-path-template (Multicast) p2mp-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]

## Example: Configuring Ingress Replication for IP Multicast Using MBGP MVPNs

- [Requirements on page 851](#)
- [Overview on page 852](#)
- [Configuration on page 853](#)
- [Verification on page 857](#)

### Requirements

The routers used in this example are Juniper Networks M Series Multiservice Edge Routers, T Series Core Routers, or MX Series 3D Universal Edge Routers running Junos OS Release 10.4 or later. When using ingress replication for IP multicast, each participating router must be configured with BGP 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, depending on the configuration of the provider tunnel in the routing instance.

## Overview

The **ingress-replication** provider tunnel type uses unicast tunnels between routers to create a multicast distribution tree.

The **mpls-internet-multicast** routing instance type uses ingress replication provider tunnels to carry IP multicast data between routers through an MPLS cloud, using MBGP (or Next Gen) MVPN. Ingress replication can also be configured when using MVPN to carry multicast data between PE routers.

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 IP multicast are associated only with the default routing instance (**inet.0**), not with a configured routing instance. The **mpls-internet-multicast** routing instance type is configured for the default master instance on each router, and is also included at the **[edit protocols pim]** hierarchy level in the default instance.

For each **mpls-internet-multicast** routing instance, the **ingress-replication** statement is required under the **provider-tunnel** statement and also under the **[edit routing-instances routing-instance-name provider-tunnel selective group source]** hierarchy level.

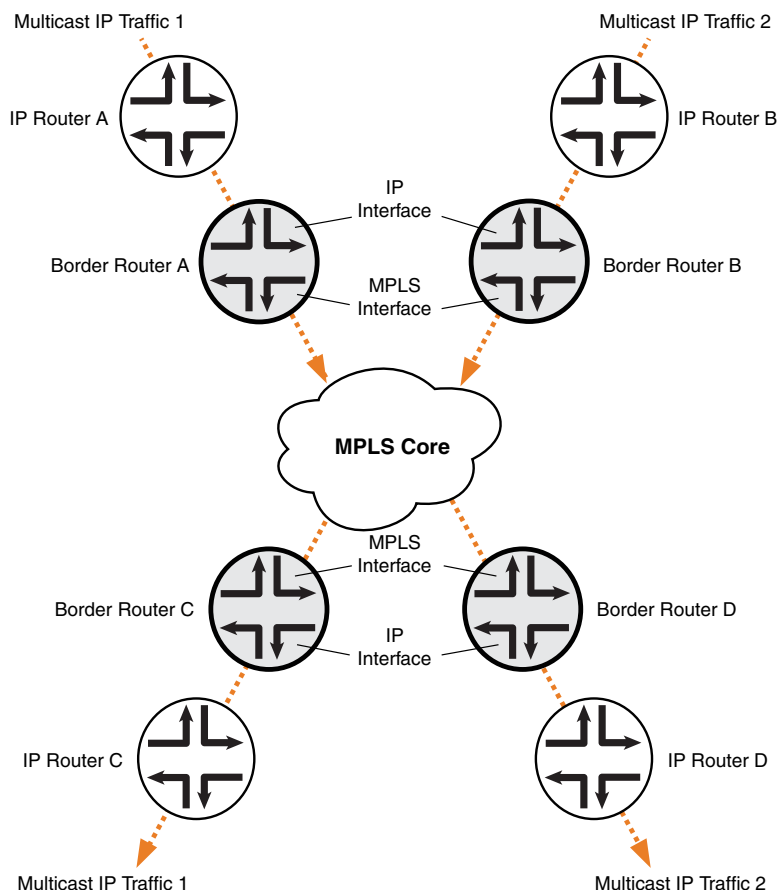
When a new destination needs to be added to the ingress replication provider tunnel, the resulting behavior differs depending on how the ingress replication provider tunnel is configured:

- **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.

The IP topology consists of routers on the edge of the IP multicast domain. Each router has a set of IP interfaces configured toward the MPLS cloud and a set of interfaces configured toward the IP routers. See [Figure 78 on page 853](#). 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 IBGP session for the control plane.



Figure 78: Internet Multicast Topology



9040632

## 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.

#### Border Router C

```
set protocols mpls ipv6-tunneling
set protocols mpls interface all
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 10.255.10.61
set protocols bgp group ibgp family inet unicast
set protocols bgp group ibgp family inet-vpn any
set protocols bgp group ibgp family inet6 unicast
set protocols bgp group ibgp family inet6-vpn any
set protocols bgp group ibgp family inet-mvpn signaling
set protocols bgp group ibgp family inet6-mvpn signaling
set protocols bgp group ibgp export to-bgp
set protocols bgp group ibgp neighbor 10.255.10.97
set protocols bgp group ibgp neighbor 10.255.10.55
set protocols bgp group ibgp neighbor 10.255.10.57
set protocols bgp group ibgp neighbor 10.255.10.59
```

```

set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface so-1/3/1.0
set protocols ospf area 0.0.0.0 interface so-0/3/0.0
set protocols ospf3 area 0.0.0.0 interface lo0.0
set protocols ospf3 area 0.0.0.0 interface so-1/3/1.0
set protocols ospf3 area 0.0.0.0 interface so-0/3/0.0
set protocols ldp interface all
set protocols pim rp static address 192.0.2.2
set protocols pim rp static address 2::192:0:2:2
set protocols pim interface fe-0/1/0.0
set protocols mpls-internet-multicast
set routing-instances test instance-type mpls-internet-multicast
set routing-instances test provider-tunnel ingress-replication label-switched-path
set routing-instances test protocols mvpn

```

**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*.

The following example shows how to configure ingress replication on an IP multicast instance with the routing instance type **mpls-internet-multicast**. Additionally, this example shows how to configure a selective provider tunnel that selects a new unicast tunnel each time a new destination needs to be added to the multicast distribution tree.

This example shows the configuration of the link between Border Router C and edge IP Router C, from which Border Router C receives PIM join messages.

1. Enable MPLS.

```

[edit protocols mpls]
user@Border_Router_C# set ipv6-tunneling
user@Border_Router_C# set interface all

```

2. Configure a signaling protocol, such as RSVP or LDP.

```

[edit protocols ldp]
user@Border_Router_C# set interface all

```

3. Configure a full-mesh of IBGP peering sessions.

```

[edit protocols bgp group ibgp]
user@Border_Router_C# set type internal
user@Border_Router_C# set local-address 10.255.10.61
user@Border_Router_C# set neighbor 10.255.10.97
user@Border_Router_C# set neighbor 10.255.10.55
user@Border_Router_C# set neighbor 10.255.10.57
user@Border_Router_C# set neighbor 10.255.10.59
user@Border_Router_C# set export to-bgp

```

4. Configure the multiprotocol BGP-related settings so that the BGP sessions carry the necessary NLRI.

```

[edit protocols bgp group ibgp]
user@Border_Router_C# set family inet unicast
user@Border_Router_C# set family inet-vpn any

```

```

user@Border_Router_C# set family inet6 unicast
user@Border_Router_C# set family inet6-vpn any
user@Border_Router_C# set family inet-mvpn signaling
user@Border_Router_C# set family inet6-mvpn signaling

```

5. Configure an interior gateway protocol (IGP).

This example shows a dual stacking configuration with OSPF and OSPF version 3 configured on the interfaces.

```

[edit protocols ospf3]
user@Border_Router_C# set area 0.0.0.0 interface lo0.0
user@Border_Router_C# set area 0.0.0.0 interface so-1/3/1.0
user@Border_Router_C# set area 0.0.0.0 interface so-0/3/0.0

```

```

[edit protocols ospf]
user@Border_Router_C# set traffic-engineering
user@Border_Router_C# set area 0.0.0.0 interface fxp0.0 disable
user@Border_Router_C# set area 0.0.0.0 interface lo0.0
user@Border_Router_C# set area 0.0.0.0 interface so-1/3/1.0
user@Border_Router_C# set area 0.0.0.0 interface so-0/3/0.0

```

6. Configure a global PIM instance on the interface facing the edge device.

PIM is not configured in the core.

```

[edit protocols pim]
user@Border_Router_C# set rp static address 192.0.2.2
user@Border_Router_C# set rp static address 2::192:0:2:2
user@Border_Router_C# set interface fe-0/1/0.0
user@Border_Router_C# set mpls-internet-multicast

```

7. Configure the ingress replication provider tunnel to create a new unicast tunnel each time a destination needs to be added to the multicast distribution tree.

```

[edit routing-instances test]
user@Border_Router_C# set instance-type mpls-internet-multicast
user@Border_Router_C# set provider-tunnel ingress-replication label-switched-path
user@Border_Router_C# set protocols mvpn

```



**NOTE:** Alternatively, use the `label-switched-path-template` statement to configure a point-to-point LSP for the ingress tunnel.

Configure the point-to-point LSP to use the default template settings (this is needed only when using RSVP tunnels). For example:

```

[edit routing-instances test provider-tunnel]
user@Border_Router_C# set ingress-replication label-switched-path
label-switched-path-template default-template
user@Border_Router_C# set selective group 203.0.113.0/24 source
192.168.195.145/32 ingress-replication label-switched-path

```

8. Commit the configuration.

```

user@Border_Router_C# commit

```

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

```
user@Border_Router_C# show protocols
mpls {
 ipv6-tunneling;
 interface all;
}
bgp {
 group ibgp {
 type internal;
 local-address 10.255.10.61;
 family inet {
 unicast;
 }
 family inet-vpn {
 any;
 }
 family inet6 {
 unicast;
 }
 family inet6-vpn {
 any;
 }
 family inet-mvpn {
 signaling;
 }
 family inet6-mvpn {
 signaling;
 }
 export to-bgp; ## 'to-bgp' is not defined
 neighbor 10.255.10.97;
 neighbor 10.255.10.55;
 neighbor 10.255.10.57;
 neighbor 10.255.10.59;
 }
}
ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface fxp0.0 {
 disable;
 }
 interface lo0.0;
 interface so-1/3/1.0;
 interface so-0/3/0.0;
 }
}
ospf3 {
 area 0.0.0.0 {
 interface lo0.0;
 interface so-1/3/1.0;
 interface so-0/3/0.0;
 }
}
```

```

}
ldp {
 interface all;
}
pim {
 rp {
 static {
 address 192.0.2.2;
 address 2::192:0:2:2;
 }
 }
 interface fe-0/1/0.0;
 mpls-internet-multicast;
}

user@Border_Router_C# show routing-instances
test {
 instance-type mpls-internet-multicast;
 provider-tunnel {
 ingress-replication {
 label-switched-path;
 }
 }
 protocols {
 mvpn;
 }
}

```

## Verification

Confirm that the configuration is working properly. The following operational output is for LDP ingress replication SPT-only mode. The multicast source behind IP Router B. The multicast receiver is behind IP Router C.

- [Checking the Ingress Replication Status on Border Router C on page 857](#)
- [Checking the Routing Table for the MVPN Routing Instance on Border Router C on page 858](#)
- [Checking the MVPN Neighbors on Border Router C on page 859](#)
- [Checking the PIM Join Status on Border Router C on page 859](#)
- [Checking the Multicast Route Status on Border Router C on page 860](#)
- [Checking the Ingress Replication Status on Border Router B on page 861](#)
- [Checking the Routing Table for the MVPN Routing Instance on Border Router B on page 861](#)
- [Checking the MVPN Neighbors on Border Router B on page 862](#)
- [Checking the PIM Join Status on Border Router B on page 863](#)
- [Checking the Multicast Route Status on Border Router B on page 863](#)

### Checking the Ingress Replication Status on Border Router C

**Purpose** Use the `show ingress-replication mvpn` command to check the ingress replication status.

**Action** user@Border\_Router\_C> show ingress-replication mvpn

```
Ingress Tunnel: mvpn:1
Application: MVPN
Unicast tunnels
 Leaf Address Tunnel-type Mode State
 10.255.10.61 P2P LSP Existing Up
```

**Meaning** The ingress replication is using a point-to-point LSP, and is in the Up state.

### Checking the Routing Table for the MVPN Routing Instance on Border Router C

**Purpose** Use the **show route table** command to check the route status.

**Action** user@Border\_Router\_C> show route table test.mvpn

```
test.mvpn.0: 5 destinations, 7 routes (5 active, 1 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1:0:0:10.255.10.61/240
 *[BGP/170] 00:45:55, localpref 100, from 10.255.10.61
 AS path: I, validation-state: unverified
 > via so-2/0/1.0
1:0:0:10.255.10.97/240
 *[MVPN/70] 00:47:19, metric2 1
 Indirect
5:0:0:32:192.168.195.106:32:198.51.100.1/240
 *[PIM/105] 00:06:35
 Multicast (IPv4) Composite
 [BGP/170] 00:06:35, localpref 100, from 10.255.10.61
 AS path: I, validation-state: unverified
 > via so-2/0/1.0
6:0:0:1000:32:192.0.2.2:32:198.51.100.1/240
 *[PIM/105] 00:07:03
 Multicast (IPv4) Composite
7:0:0:1000:32:192.168.195.106:32:198.51.100.1/240
 *[MVPN/70] 00:06:35, metric2 1
 Multicast (IPv4) Composite
 [PIM/105] 00:05:35
 Multicast (IPv4) Composite

test.mvpn-inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1:0:0:10.255.10.61/432
 *[BGP/170] 00:45:55, localpref 100, from 10.255.10.61
 AS path: I, validation-state: unverified
 > via so-2/0/1.0
1:0:0:10.255.10.97/432
 *[MVPN/70] 00:47:19, metric2 1
 Indirect
```

**Meaning** The expected routes are populating the test.mvpn routing table.

### Checking the MVPN Neighbors on Border Router C

**Purpose** Use the `show mvpn neighbor` command to check the neighbor status.

**Action** `user@Border_Router_C> show mvpn neighbor`

```
MVPN instance:
Legend for provider tunnel
S- Selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g) RM -- remote VPN route
Family : INET

Instance : test
 MVPN Mode : SPT-ONLY
 Neighbor Inclusive Provider Tunnel
 10.255.10.61 INGRESS-REPLICATION:MPLS Label
 16:10.255.10.61

MVPN instance:
Legend for provider tunnel
S- Selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g) RM -- remote VPN route
Family : INET6

Instance : test
 MVPN Mode : SPT-ONLY
 Neighbor Inclusive Provider Tunnel
 10.255.10.61 INGRESS-REPLICATION:MPLS Label
 16:10.255.10.61
```

### Checking the PIM Join Status on Border Router C

**Purpose** Use the `show pim join extensive` command to check the PIM join status.

**Action**    user@Border\_Router\_C> show pim join extensive  
Instance: PIM.master Family: INET  
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 198.51.100.1  
Source: \*  
RP: 192.0.2.2  
Flags: sparse,rptree,wildcard  
Upstream interface: Local  
Upstream neighbor: Local  
Upstream state: Local RP  
Uptime: 00:07:49  
Downstream neighbors:  
  Interface: ge-3/0/6.0  
    192.0.2.2 State: Join Flags: SRW Timeout: Infinity  
    Uptime: 00:07:49 Time since last Join: 00:07:49  
  Number of downstream interfaces: 1

Group: 198.51.100.1  
Source: 192.168.195.106  
Flags: sparse  
Upstream protocol: BGP  
Upstream interface: Through BGP  
Upstream neighbor: Through MVPN  
Upstream state: Local RP, Join to Source, No Prune to RP  
Keepalive timeout: 69  
Uptime: 00:06:21  
Number of downstream interfaces: 0

Instance: PIM.master Family: INET6  
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

---

### Checking the Multicast Route Status on Border Router C

**Purpose**    Use the **show multicast route extensive** command to check the multicast route status.



**Action** user@Border\_Router\_C> **show multicast route extensive**  
 Instance: master Family: INET

Group: 198.51.100.1  
 Source: 192.168.195.106/32  
 Upstream interface: lsi.0  
 Downstream interface list:  
     ge-3/0/6.0  
 Number of outgoing interfaces: 1  
 Session description: NOB Cross media facilities  
 Statistics: 18 kbps, 200 pps, 88907 packets  
 Next-hop ID: 1048577  
 Upstream protocol: MVPN  
 Route state: Active  
 Forwarding state: Forwarding  
 Cache lifetime/timeout: forever  
 Wrong incoming interface notifications: 0  
 Uptime: 00:07:25

Instance: master Family: INET6

### Checking the Ingress Replication Status on Border Router B

**Purpose** Use the **show ingress-replication mvpn** command to check the ingress replication status.

**Action** user@Border\_Router\_B> **show ingress-replication mvpn**

Ingress Tunnel: mvpn:1  
 Application: MVPN  
 Unicast tunnels

| Leaf Address | Tunnel-type | Mode     | State |
|--------------|-------------|----------|-------|
| 10.255.10.97 | P2P LSP     | Existing | Up    |

**Meaning** The ingress replication is using a point-to-point LSP, and is in the Up state.

### Checking the Routing Table for the MVPN Routing Instance on Border Router B

**Purpose** Use the **show route table** command to check the route status.

**Action** user@Border\_Router\_B> show route table test.mvpn

```
test.mvpn.0: 5 destinations, 7 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1:0:0:10.255.10.61/240
 *[MVPN/70] 00:49:26, metric2 1
 Indirect
1:0:0:10.255.10.97/240
 *[BGP/170] 00:48:22, localpref 100, from 10.255.10.97
 AS path: I, validation-state: unverified
 > via so-1/3/1.0
5:0:0:32:192.168.195.106:32:198.51.100.1/240
 *[PIM/105] 00:09:02
 Multicast (IPv4) Composite
 [BGP/170] 00:09:02, localpref 100, from 10.255.10.97
 AS path: I, validation-state: unverified
 > via so-1/3/1.0
7:0:0:1000:32:192.168.195.106:32:198.51.100.1/240
 *[PIM/105] 00:09:02
 Multicast (IPv4) Composite
 [BGP/170] 00:09:02, localpref 100, from 10.255.10.97
 AS path: I, validation-state: unverified
 > via so-1/3/1.0

test.mvpn-inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1:0:0:10.255.10.61/432
 *[MVPN/70] 00:49:26, metric2 1
 Indirect
1:0:0:10.255.10.97/432
 *[BGP/170] 00:48:22, localpref 100, from 10.255.10.97
 AS path: I, validation-state: unverified
 > via so-1/3/1.0
```

**Meaning** The expected routes are populating the test.mvpn routing table.

---

### Checking the MVPN Neighbors on Border Router B

---

**Purpose** Use the show mvpn neighbor command to check the neighbor status.

**Action** user@Border\_Router\_B> show mvpn neighbor

```

MVPN instance:
Legend for provider tunnel
S- Selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g) RM -- remote VPN route
Family : INET

Instance : test
 MVPN Mode : SPT-ONLY
 Neighbor Inclusive Provider Tunnel
 10.255.10.97 INGRESS-REPLICATION:MPLS Label
 16:10.255.10.97

MVPN instance:
Legend for provider tunnel
S- Selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g) RM -- remote VPN route
Family : INET6

Instance : test
 MVPN Mode : SPT-ONLY
 Neighbor Inclusive Provider Tunnel
 10.255.10.97 INGRESS-REPLICATION:MPLS Label
 16:10.255.10.97

```

### Checking the PIM Join Status on Border Router B

**Purpose** Use the `show pim join extensive` command to check the PIM join status.

**Action** user@Border\_Router\_B> show pim join extensive  
 Instance: PIM.master Family: INET  
 R = Rendezvous Point Tree, S = Sparse, W = Wildcard

```

Group: 198.51.100.1
 Source: 192.168.195.106
 Flags: sparse,spt
 Upstream interface: fe-0/1/0.0
 Upstream neighbor: Direct
 Upstream state: Local Source
 Keepalive timeout: 0
 Uptime: 00:09:39
 Downstream neighbors:
 Interface: Pseudo-MVPN
 Uptime: 00:09:39 Time since last Join: 00:09:39
 Number of downstream interfaces: 1

```

```

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

```

### Checking the Multicast Route Status on Border Router B

**Purpose** Use the `show multicast route extensive` command to check the multicast route status.

**Action**    user@Border\_Router\_B> show multicast route extensive  
Instance: master Family: INET

Group: 198.51.100.1  
Source: 192.168.195.106/32  
Upstream interface: fe-0/1/0.0  
Downstream interface list:  
    so-1/3/1.0  
Number of outgoing interfaces: 1  
Session description: NOB Cross media facilities  
Statistics: 18 kbps, 200 pps, 116531 packets  
Next-hop ID: 1048580  
Upstream protocol: MVPN  
Route state: Active  
Forwarding state: Forwarding  
Cache lifetime/timeout: forever  
Wrong incoming interface notifications: 0  
Uptime: 00:09:43

- Related Documentation**
- *Configuring Routing Instances for an MBGP MVPN*
  - *mpls-internet-multicast*
  - *ingress-replication*
  - *create-new-ucast-tunnel*
  - [label-switched-path-template \(Multicast\) on page 1135](#)
  - *show ingress-replication mvpn*

---

## Mapping VPLS Traffic to Specific LSPs

You can map VPLS traffic to specific LSPs by configuring forwarding table policies. This procedure is optional but can be useful. The following example illustrates how you can map lower priority VPLS routing instances to slower LSPs while mapping other higher priority VPLS routing instances to faster LSPs. In this example configuration, **a-to-b1** and **a-to-c1** are high-priority LSPs between the PE routers, while **a-to-b2** and **a-to-c2** are low-priority LSPs between the PE routers.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

---

To map VPLS traffic, include the **policy-statement vpls-priority** statement:

```
policy-statement vpls-priority {
 term a {
 from {
 rib mpls.0;
 community company-1;
 }
 then {
```

```

 install-nexthop lsp [a-to-b1 a-to-c1];
 accept;
 }
}
term b {
 from {
 rib mpls.0;
 community company-2;
 }
 then {
 install-nexthop lsp-regex ["^a-to-b2$" "^a-to-c2$"];
 accept;
 }
}
}
community company-1 members target:11111:1;
community company-2 members target:11111:2;

```

You can include the **policy-statement vpls-priority** statement at the following hierarchy levels:

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

Include the **export** statement to apply the **vpls-priority** policy to the forwarding table:

```
export vpls-priority;
```

You can include this statement at the following hierarchy levels:

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

For more information about how to configure routing policies, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*.



# Configuring Inter-AS VPLS and IRB VPLS

- [Example: Configuring Inter-AS VPLS with MAC Processing at the ASBR on page 867](#)
- [Configuring VPLS and Integrated Routing and Bridging on page 892](#)

## Example: Configuring Inter-AS VPLS with MAC Processing at the ASBR

---

This example describes how to configure inter-AS Virtual Private LAN Service (VPLS) with MAC processing between BGP-signaled VPLS and LDP-signaled VPLS. This feature is described in RFC 4761 as multi-AS VPLS option E or method E.

This example is organized in the following sections:

- [Requirements on page 867](#)
- [Overview and Topology on page 867](#)
- [Configuration on page 869](#)

### Requirements

To support inter-AS VPLS between BGP-signaled VPLS and LDP-signaled VPLS, your network must meet the following hardware and software requirements:

- MX Series or M320 routers for the ASBRs.
- Junos OS Release 9.3 or higher.
- Gigabit Ethernet or 10-Gigabit Ethernet interfaces.

### Overview and Topology

VPLS is a key enabler for delivering multipoint Ethernet service. Major service providers have implemented IP and MPLS backbones and offer VPLS services to large enterprises. Growing demand requires the VPLS network to scale to support many VPLS customers with multiple sites spread across geographically dispersed regions. BGP-signaled VPLS signaling offers scaling advantages over LDP-signaled VPLS. In some environments there is a need for BGP-signaled VPLS to interoperate with existing LDP-signaled VPLS.

This example shows one way to configure BGP-signaled VPLS interworking with an existing LDP-signaled VPLS network.

The advantages of the configuration are:

- You can interconnect customer sites that are spread across different autonomous systems (ASs).
- LDP-signaled VPLS and BGP-signaled VPLS interworking is supported.
- Because the ASBR supports MAC operations, customer sites can be connected directly to the ASBR.
- The inter-AS link is not restricted to Ethernet interfaces.
- Additional configuration for multihoming is relatively straightforward.

Traffic from the interworking virtual private LAN services is switched at the ASBR. The ASBR does all the data plane operations: flooding, MAC learning, aging, and MAC forwarding for each AS to switch traffic among any customer facing interfaces and between the fully meshed pseudowires in the AS. A single pseudowire is created between the ASBRs across the inter-AS link and the ASBRs forward traffic from the pseudowires in each AS to the peer ASBR.

Each ASBR performs VPLS operations within its own AS and performs VPLS operations with the ASBR in the other AS. The ASBR treats the other AS as a BGP-signaled VPLS site. To establish VPLS pseudowires, VPLS NLRI messages are exchanged across the EBGP sessions on the inter-AS links between the ASBRs.

The sample metro network is configured for LDP-signaled VPLS. The core network is configured for BGP-signaled VPLS.

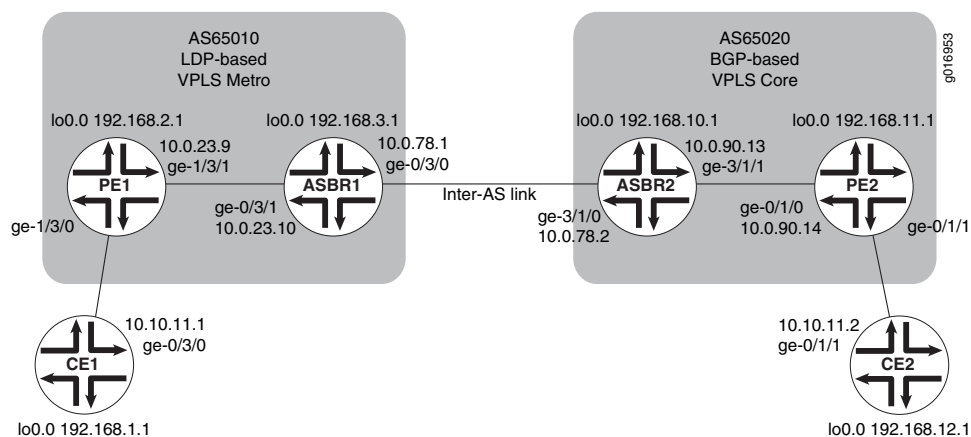
The first part of the example shows the basic configuration steps to configure the logical interfaces, OSPF, internal BGP, LDP, and MPLS. This part of the configuration is the same as other VPLS configurations for LDP-signaled VPLS and BGP-signaled VPLS.

The unique part of the example is configured in the VPLS routing instances, external BGP, and the policy that populates the BGP route table with routes learned from direct routes and OSPF routes. Additional details about the configuration statements are included in the step-by-step procedure.

[Figure 79 on page 869](#) shows the topology used in this example.



Figure 79: Inter-AS VPLS with MAC Operations Example Topology



## Configuration

To configure inter-AS VPLS between BGP-signaled VPLS and LDP-signaled VPLS, perform these tasks.



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

- [Configuring Interfaces on page 869](#)
- [Configuring OSPF on page 871](#)
- [Configuring the Internal BGP Peer Group on page 872](#)
- [Configuring LDP on page 873](#)
- [Configuring MPLS on page 874](#)
- [Configuring the External BGP Peer Group Between the Loopback Interfaces on page 875](#)
- [Configuring the External BGP Peer Group Between the Inter-AS Link Interfaces on page 875](#)
- [Configuring the VPLS Routing Instances on page 879](#)
- [Results on page 883](#)

### Configuring Interfaces

#### Step-by-Step Procedure

To configure interfaces:

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

```
user@CE1# set interfaces lo0 unit 0 family inet address 192.168.1.1/32 primary
```

```
user@PE1# set interfaces lo0 unit 0 family inet address 192.168.2.1/32 primary
```

```
user@ASBR1# set interfaces lo0 unit 0 family inet address 192.168.3.1/32 primary
```

```
user@ASBR2# set interfaces lo0 unit 0 family inet address 192.168.10.1/32 primary
```

```
user@PE2# set interfaces lo0 unit 0 family inet address 192.168.11.1/32 primary
```

```
user@CE2# set interfaces lo0 unit 0 family inet address 192.168.12.1/32 primary
```

2. On each router, commit the configuration:

```
user@host> commit check
configuration check succeeds
user@host> commit
commit complete
```

3. On each router, display the interface information for **lo0** and verify that the correct IP address is configured:

```
user@host> show interfaces lo0
```

```
Physical interface: lo0, Enabled, Physical link is Up
 Interface index: 6, SNMP ifIndex: 6
 Type: Loopback, MTU: Unlimited
 Device flags : Present Running Loopback
 Interface flags: SNMP-Traps
 Link flags : None
 Last flapped : Never
 Input packets : 0
 Output packets: 0
```

```
Logical interface lo0.0 (Index 75) (SNMP ifIndex 16)
 Flags: SNMP-Traps Encapsulation: Unspecified
 Input packets : 0
 Output packets: 0
 Protocol inet, MTU: Unlimited
 Flags: None
 Addresses
 Local: 127.0.0.1
 Addresses, Flags: Primary Is-Default Is-Primary
 Local: 192.168.3.1
Logical interface lo0.16384 (Index 64) (SNMP ifIndex 21)
 Flags: SNMP-Traps Encapsulation: Unspecified
 Input packets : 0
 Output packets: 0
 Protocol inet, MTU: Unlimited
 Flags: None
 Addresses
 Local: 127.0.0.1
```

```
Logical interface lo0.16385 (Index 65) (SNMP ifIndex 22)
 Flags: SNMP-Traps Encapsulation: Unspecified
 Input packets : 0
 Output packets: 0
 Protocol inet, MTU: Unlimited
 Flags: None
```

In the example above notice that the primary **lo0** local address for the **inet** protocol family on Router ASBR1 is **192:168:3:1**.

4. On each router, configure an IP address and protocol family on the Gigabit Ethernet interfaces. Specify the **inet** protocol family.

```
user@CE1# set interfaces ge-0/3/0 unit 0 family inet address 10.10.11.1/24
```

```
user@PE1# set interfaces ge-1/3/1 unit 0 family inet address 10.0.23.9/30
```

```
user@ASBR1# set interfaces ge-0/3/1 unit 0 family inet address 10.0.23.10/30
user@ASBR1# set interfaces ge-0/3/0 unit 0 family inet address 10.0.78.1/30
```

```
user@ASBR2# set interfaces ge-3/1/0 unit 0 family inet address 10.0.78.2/30
user@ASBR2# set interfaces ge-3/1/1 unit 0 family inet address 10.0.90.13/30
```

```
user@PE2# set interfaces ge-0/1/0 unit 0 family inet address 10.0.90.14/30
```

```
user@CE2# set interfaces ge-0/1/1 unit 0 family inet address 10.10.11.2/24
```

5. On each router, commit the configuration:

```
user@host> commit check
configuration check succeeds
user@host> commit
commit complete
```

6. Display information for Gigabit Ethernet interfaces and verify that the IP address and protocol family are configured correctly.

```
user@ASBR2> show interfaces ge-* terse
```

| Interface  | Admin | Link | Proto | Local         | Remote |
|------------|-------|------|-------|---------------|--------|
| ge-3/1/0   | up    | up   |       |               |        |
| ge-3/1/0.0 | up    | up   | inet  | 10.0.78.2/30  |        |
|            |       |      |       | multiservice  |        |
| ge-3/1/1   | up    | up   |       |               |        |
| ge-3/1/1.0 | up    | up   | inet  | 10.0.90.13/30 |        |
|            |       |      |       | multiservice  |        |
| ge-3/1/2   | up    | down |       |               |        |
| ge-3/1/3   | up    | down |       |               |        |

## Configuring OSPF

### Step-by-Step Procedure

To configure OSPF:

1. On the PE and ASBR routers, configure the provider instance of OSPF. Configure OSPF traffic engineering support. Specify area 0.0.0.1 in the LDP-signaled VPLS network and area 0.0.0.0 in the BGP-signaled network. Specify the Gigabit Ethernet logical interfaces between the PE and ASBR routers. Specify **lo0.0** as a passive interface.

```
user@PE1# set protocols ospf traffic-engineering
user@PE1# set protocols ospf area 0.0.0.1 interface ge-1/3/1.0
user@PE1# set protocols ospf area 0.0.0.1 interface lo0.0 passive
```

```
user@ASBR1# set protocols ospf traffic-engineering
user@ASBR1# set protocols ospf area 0.0.0.1 interface ge-0/3/1.0
user@ASBR1# set protocols ospf area 0.0.0.1 interface lo0.0 passive
```

```
user@ASBR2# set protocols ospf traffic-engineering
user@ASBR2# set protocols ospf area 0.0.0.0 interface ge-3/1/1.0
user@ASBR2# set protocols ospf area 0.0.0.0 interface lo0.0 passive
```

```
user@PE2# set protocols ospf traffic-engineering
user@PE2# set protocols ospf area 0.0.0.0 interface ge-0/1/0.0
user@PE2# set protocols ospf area 0.0.0.0 interface lo0.0 passive
```

2. On each router, commit the configuration:

```
user@host> commit check
configuration check succeeds
user@host> commit
commit complete
```

3. Display OSPF neighbor information and verify that the PE routers form adjacencies with the ASBR router in the same area. Verify that the neighbor state is **Full**.

```
user@host> show ospf neighbor
Address Interface State ID Pri Dead
10.0.23.10 ge-1/3/1.0 Full 192.168.3.1 128 31
```

### Configuring the Internal BGP Peer Group

#### Step-by-Step Procedure

The purpose of configuring an internal BGP peer group is to create a full mesh of BGP LSPs among the PE routers in the BGP-signaled AS, including the ASBR routers.

To configure the internal BGP peer group:

1. The purpose of this step is to create a full mesh of IBGP peers between the PE routers, including the ASBR routers, within the BGP-signaled AS.

On Router ASBR2, configure internal BGP. Specify the BGP type as **internal**. Specify the local address as the local **lo0** IP address.

Specify the **inet** protocol family. Specify the **labeled-unicast** statement and the **resolve-vpn** option. The **labeled-unicast** statement causes the router to advertise labeled routes out of the IPv4 inet.0 route table and places labeled routes into the inet.0 route table. The **resolve-vpn** option puts labeled routes in the MPLS inet.3 route table. The inet.3 route table is used to resolve routes for the PE router located in the other AS.

Specify the **l2vpn** family to indicate to the router that this is a VPLS. Specify the **signaling** option to configure BGP as the signaling protocol. This enables BGP to carry Layer 2 VPLS NLRI messages for this peer group.

Specify the **lo0** interface IP address of the PE as the neighbor. Configure an autonomous system identifier.

```
user@ASBR2# set protocols bgp group core-ibgp type internal
user@ASBR2# set protocols bgp group core-ibgp local-address 192.168.10.1
user@ASBR2# set protocols bgp group core-ibgp family inet labeled-unicast
resolve-vpn
user@ASBR2# set protocols bgp group core-ibgp family l2vpn signaling
user@ASBR2# set protocols bgp group core-ibgp neighbor 192.168.11.1
user@ASBR2# set routing-options autonomous-system 0.65020
```

2. On Router PE2, configure internal BGP. Specify the BGP type as **internal**. Specify the local address as the local **lo0** IP address.

Specify the **l2vpn** family to indicate this is a VPLS. Specify the **signaling** option to configure BGP as the signaling protocol. This enables BGP to carry Layer 2 VPLS NLRI messages.

Specify the **lo0** interface IP address of Router ASBR2 as the neighbor. Configure an autonomous system identifier.

```

user@PE2# set protocols bgp group core-ibgp type internal
user@PE2# set protocols bgp group core-ibgp local-address 192.168.11.1
user@PE2# set protocols bgp group core-ibgp family l2vpn signaling
user@PE2# set protocols bgp group core-ibgp neighbor 192.168.10.1
user@PE2# set routing-options autonomous-system 0.65020

```

3. On each router, commit the configuration:

```

user@host> commit check
configuration check succeeds
user@host> commit
commit complete

```

4. On Router PE2 and Router ASBR2, display BGP neighbor information and verify that the peer connection state is **Established**.

```

user@ASBR2> show bgp neighbor
Peer: 192.168.11.1+49443 AS 65020 Local: 192.168.10.1+179 AS 65020
 Type: Internal State: Established Flags: ImportEval Sync
 Last State: OpenConfirm Last Event: RecvKeepAlive
 Last Error: None
 Options: Preference LocalAddress AddressFamily Rib-group Refresh
 Address families configured: l2vpn-signaling inet-labeled-unicast
 Local Address: 192.168.10.1 Holdtime: 90 Preference: 170
 Number of flaps: 0
 Peer ID: 192.168.11.1 Local ID: 192.168.10.1 Active Holdtime: 90
 Keepalive Interval: 30 Peer index: 0

```

...

## Configuring LDP

### Step-by-Step Procedure

To configure LDP:

1. On the PE and ASBR routers, configure LDP with the Gigabit Ethernet interfaces between the PE and ASBR routers, and between the two ASBR routers. To support LDP-signaled VPLS, additionally configure LDP with the **lo0.0** interface on Router PE1 and Router ASBR1:

```

user@PE1# set protocols ldp interface ge-1/3/1.0
user@PE1# set protocols ldp interface lo0.0

```

```

user@ASBR1# set protocols ldp interface ge-0/3/1.0
user@ASBR1# set protocols ldp interface ge-0/3/0.0
user@ASBR1# set protocols ldp interface lo0.0

```

```

user@ASBR2# set protocols ldp interface ge-3/1/0.0
user@ASBR2# set protocols ldp interface ge-3/1/1.0

```

```

user@PE2# set protocols ldp interface ge-0/1/0.0

```



**NOTE:** The configuration of LDP signaling between the ASBR routers is not required for Inter-AS VPLS. It is included here for reference only and might be used in LDP environments.

2. On each router, commit the configuration:

```
user@host> commit check
configuration check succeeds
user@host> commit
commit complete
```

3. Display LDP configuration information and verify that the correct interfaces are configured. LDP operation can be verified after MPLS is configured.

```
user@ASBR1> show configuration protocols ldp
interface ge-0/3/0.0;
interface ge-0/3/1.0;
interface lo0.0;
```

The preceding example is from ASBR1.

### Configuring MPLS

#### Step-by-Step Procedure

To configure MPLS:

1. On the PE and ASBR routers, configure MPLS. Enable MPLS on the logical interfaces. Add the Gigabit Ethernet interfaces to the MPLS protocol. This adds entries to the MPLS forwarding table.

```
user@PE1# set protocols mpls interface ge-1/3/1.0
user@PE1# set interfaces ge-1/3/1 unit 0 family mpls
```

```
user@ASBR1# set protocols mpls interface ge-0/3/1.0
user@ASBR1# set protocols mpls interface ge-0/3/0.0
user@ASBR1# set interfaces ge-0/3/1 unit 0 family mpls
user@ASBR1# set interfaces ge-0/3/0 unit 0 family mpls
```

```
user@ASBR2# set protocols mpls interface ge-3/1/0.0
user@ASBR2# set protocols mpls interface ge-3/1/1.0
user@ASBR2# set interfaces ge-3/1/0 unit 0 family mpls
user@ASBR2# set interfaces ge-3/1/1 unit 0 family mpls
```

```
user@PE2# set protocols mpls interface ge-0/1/0.0
user@PE2# set interfaces ge-0/1/0 unit 0 family mpls
```

2. On each router, commit the configuration:

```
user@host> commit check
configuration check succeeds
user@host> commit
commit complete
```

3. On the PE and ASBR routers, display LDP neighbor information and verify that the directly connected LDP neighbors are listed:

```
user@ASBR1> show ldp neighbor
```

| Address     | Interface  | Label space ID | Hold time |
|-------------|------------|----------------|-----------|
| 192.168.2.1 | lo0.0      | 192.168.2.1:0  | 44        |
| 10.0.78.2   | ge-0/3/0.0 | 192.168.10.1:0 | 13        |
| 10.0.23.9   | ge-0/3/1.0 | 192.168.2.1:0  | 11        |

The preceding example is from ASBR1.

### Configuring the External BGP Peer Group Between the Loopback Interfaces

#### Step-by-Step Procedure

To configure the external BGP (EBGP) peer group between the loopback interfaces:

1. On Router ASBR1 and Router PE1, configure an autonomous system identifier:  

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

```
user@ASBR1# set routing-options autonomous-system 0.65010
```
2. On Router ASBR1, configure an external BGP peer group for the loopback interfaces. Specify the **external** BGP group type. Include the **multihop** statement. Specify the local address as the local **lo0** IP address. Configure the **l2vpn** family for BGP signaling. Configure the peer AS as the core AS number. Specify the **lo0** IP address of Router ASBR2 as the neighbor.  

```
user@ASBR1# set protocols bgp group vpls-core type external
user@ASBR1# set protocols bgp group vpls-core multihop
user@ASBR1# set protocols bgp group vpls-core local-address 192.168.3.1
user@ASBR1# set protocols bgp group vpls-core family l2vpn signaling
user@ASBR1# set protocols bgp group vpls-core peer-as 65020
user@ASBR1# set protocols bgp group vpls-core neighbor 192.168.10.1
```
3. On Router ASBR2, configure an external BGP peer group for the loopback interfaces. Specify the **external** BGP group type. Include the **multihop** statement. The **multihop** statement is needed because the EBGP neighbors are in different ASs. Specify the local address as the local **lo0** IP address. Configure the **l2vpn** family for BGP signaling. Configure the peer AS as the metro AS number. Specify the **lo0** IP address of Router ASBR1 as the neighbor.  

```
user@ASBR2# set protocols bgp group vpls-metro type external
user@ASBR2# set protocols bgp group vpls-metro multihop
user@ASBR2# set protocols bgp group vpls-metro local-address 192.168.10.1
user@ASBR2# set protocols bgp group vpls-metro family l2vpn signaling
user@ASBR2# set protocols bgp group vpls-metro peer-as 65010
user@ASBR2# set protocols bgp group vpls-metro neighbor 192.168.3.1
```
4. On each router, commit the configuration:  

```
user@host> commit
```

### Configuring the External BGP Peer Group Between the Inter-AS Link Interfaces

#### Step-by-Step Procedure

The purpose of configuring external BGP peer groups between the inter-AS link interfaces is to create a full mesh of BGP LSPs among the ASBR routers. To configure the external BGP peer group between the inter-AS link interfaces:

1. On Router ASBR1, configure a policy to export OSPF and direct routes, including the **lo0** address of the PE routers, into BGP for the establishment of label-switched paths (LSPs):  

```
user@ASBR1# set policy-options policy-statement loopback term term1 from protocol ospf
user@ASBR1# set policy-options policy-statement loopback term term1 from protocol direct
```

```

user@ASBR1# set policy-options policy-statement loopback term term1 from
route-filter 192.168.0.0/16 longer
user@ASBR1# set policy-options policy-statement loopback term term1 then accept

```

2. On Router ASBR1, configure an external BGP peer group for the inter-AS link. Specify the **external** BGP group type. Specify the local inter-AS link IP address as the local address. Configure the **inet** family and include the **labeled-unicast** and **resolve-vpn** statements. The **labeled-unicast** statement advertises labeled routes out of the IPv4 inet.0 route table and places labeled routes into the inet.0 route table. The **resolve-vpn** option stores labeled routes in the MPLS **inet.3** route table.

Include the **export** statement and specify the policy you created. Configure the peer AS as the core AS number. Specify the inter-AS link IP address of Router ASBR2 as the neighbor.

```

user@ASBR1# set protocols bgp group metro-core type external
user@ASBR1# set protocols bgp group metro-core local-address 10.0.78.1
user@ASBR1# set protocols bgp group metro-core family inet labeled-unicast
resolve-vpn
user@ASBR1# set protocols bgp group metro-core export loopback
user@ASBR1# set protocols bgp group metro-core peer-as 65020
user@ASBR1# set protocols bgp group metro-core neighbor 10.0.78.2

```

3. On Router ASBR2, configure a policy to export OSPF and direct routes, including the **lo0** address, into BGP for the establishment of LSPs:

```

user@ASBR2# set policy-options policy-statement loopback term term1 from
protocol ospf
user@ASBR2# set policy-options policy-statement loopback term term1 from
protocol direct
user@ASBR2# set policy-options policy-statement loopback term term1 from
route-filter 192.168.0.0/16 longer
user@ASBR2# set policy-options policy-statement loopback term term1 then accept

```

4. On Router ASBR2, configure an external BGP peer group for the inter-AS link. Specify the **external** BGP group type. Specify the local inter-AS link IP address as the local address. Configure the **inet** family and include the **labeled-unicast** and **resolve-vpn** statements. Include the **export** statement and specify the policy you created. Configure the peer AS as the core AS number. Specify the inter-AS link IP address of Router ASBR1 as the neighbor.

```

user@ASBR2# set protocols bgp group core-metro type external
user@ASBR2# set protocols bgp group core-metro local-address 10.0.78.2
user@ASBR2# set protocols bgp group core-metro family inet labeled-unicast
resolve-vpn
user@ASBR2# set protocols bgp group core-metro export loopback
user@ASBR2# set protocols bgp group core-metro peer-as 65010
user@ASBR2# set protocols bgp group core-metro neighbor 10.0.78.1

```

5. On each router, commit the configuration:

```

user@host> commit check
configuration check succeeds
user@host> commit
commit complete

```

6. On Router ASBR1, display the BGP neighbors. Verify that the first peer is the IP address of the Gigabit Ethernet interface of Router ASBR2. Verify that the second



peer is the IP address of the **lo0** interface of Router ASBR2. Also verify that the state of each peer is **Established**. Notice that on Router ASBR1 the NLRI advertised by Router ASBR2 the inter-AS link peer is **inet-labeled-unicast** and the NLRI advertised by Router ASBR2 the loopback interface peer is **l2vpn-signaling**.

```
user@ASBR1> show bgp neighbor
```

```
Peer: 10.0.78.2+65473 AS 65020 Local: 10.0.78.1+179 AS 65010
 Type: External State: Established Flags: Sync
 Last State: OpenConfirm Last Event: RecvKeepAlive
 Last Error: Cease
 Export: [loopback]
 Options: Preference LocalAddress AddressFamily PeerAS Rib-group Refresh
 Address families configured: inet-labeled-unicast
 Local Address: 10.0.78.1 Holdtime: 90 Preference: 170
 Number of flaps: 3
 Last flap event: Stop
 Error: 'Cease' Sent: 1 Recv: 2
 Peer ID: 192.168.10.1 Local ID: 192.168.3.1 Active Holdtime: 90
 Keepalive Interval: 30 Peer index: 0
 BFD: disabled, down
 Local Interface: ge-0/3/0.0
 NLRI for restart configured on peer: inet-labeled-unicast
 NLRI advertised by peer: inet-labeled-unicast
 NLRI for this session: inet-labeled-unicast
 Peer supports Refresh capability (2)
 Restart time configured on the peer: 120
 Stale routes from peer are kept for: 300
 Restart time requested by this peer: 120
 NLRI that peer supports restart for: inet-labeled-unicast
 NLRI that restart is negotiated for: inet-labeled-unicast
 NLRI of received end-of-rib markers: inet-labeled-unicast
 NLRI of all end-of-rib markers sent: inet-labeled-unicast
 Peer supports 4 byte AS extension (peer-as 65020)
 Table inet.0 Bit: 10000
 RIB State: BGP restart is complete
 Send state: in sync
 Active prefixes: 2
 Received prefixes: 3
 Accepted prefixes: 3
 Suppressed due to damping: 0
 Advertised prefixes: 3
 Last traffic (seconds): Received 8 Sent 3 Checked 60
 Input messages: Total 8713 Updates 3 Refreshes 0 Octets 165688
 Output messages: Total 8745 Updates 2 Refreshes 0 Octets 166315
 Output Queue[0]: 0

Peer: 192.168.10.1+51234 AS 65020 Local: 192.168.3.1+179 AS 65010
 Type: External State: Established Flags: Sync
 Last State: OpenConfirm Last Event: RecvKeepAlive
 Last Error: Cease
 Options: Multihop Preference LocalAddress AddressFamily PeerAS Rib-group Refresh
 Address families configured: l2vpn-signaling
 Local Address: 192.168.3.1 Holdtime: 90 Preference: 170
 Number of flaps: 3
 Last flap event: Stop
 Error: 'Cease' Sent: 1 Recv: 2
 Peer ID: 192.168.10.1 Local ID: 192.168.3.1 Active Holdtime: 90
 Keepalive Interval: 30 Peer index: 0
 BFD: disabled, down
 NLRI for restart configured on peer: l2vpn-signaling
```

```

NLRI advertised by peer: l2vpn-signaling
NLRI for this session: l2vpn-signaling
Peer supports Refresh capability (2)
Restart time configured on the peer: 120
Stale routes from peer are kept for: 300
Restart time requested by this peer: 120
NLRI that peer supports restart for: l2vpn-signaling
NLRI that restart is negotiated for: l2vpn-signaling
NLRI of received end-of-rib markers: l2vpn-signaling
NLRI of all end-of-rib markers sent: l2vpn-signaling
Peer supports 4 byte AS extension (peer-as 65020)
Table bgp.l2vpn.0 Bit: 20000
 RIB State: BGP restart is complete
 RIB State: VPN restart is complete
 Send state: in sync
 Active prefixes: 1
 Received prefixes: 1
 Accepted prefixes: 1
 Suppressed due to damping: 0
 Advertised prefixes: 1
Table inter-as.l2vpn.0
 RIB State: BGP restart is complete
 RIB State: VPN restart is complete
 Send state: not advertising
 Active prefixes: 1
 Received prefixes: 1
 Accepted prefixes: 1
 Suppressed due to damping: 0
Last traffic (seconds): Received 19 Sent 18 Checked 42
Input messages: Total 8712 Updates 3 Refreshes 0 Octets 165715
Output messages: Total 8744 Updates 2 Refreshes 0 Octets 166342
Output Queue[1]: 0
Output Queue[2]: 0

```

7. On Router ASBR2, display the BGP summary. Notice that the first peer is the IP address of the Gigabit Ethernet interface of Router ASBR1, the second peer is the IP address of the **lo0** interface of Router ASBR1, and the third peer is the **lo0** interface of Router PE2. Verify that the state of each peer is **Established**.

```

user@ASBR2> show bgp summary
Groups: 3 Peers: 3 Down peers: 0
Table Tot Paths Act Paths Suppressed History Damp State Pending
inet.0 3 2 0 0 0 0 0
bgp.l2vpn.0 2 2 0 0 0 0 0
Peer AS InPkt OutPkt OutQ Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
10.0.78.1 65010 8781 8748 0 2 2d 17:54:56 Establ
 inet.0: 2/3/3/0
192.168.3.1 65010 8780 8747 0 2 2d 17:54:54 Establ
 bgp.l2vpn.0: 1/1/1/0
 inter-as.l2vpn.0: 1/1/1/0
192.168.11.1 65020 8809 8763 0 1 2d 17:59:22 Establ
 bgp.l2vpn.0: 1/1/1/0
 inter-as.l2vpn.0: 1/1/1/0

```

8. On Router PE2, display the BGP group. Verify that the peer is the IP address of the **lo0** interface of Router ASBR2. Verify that the number of established peer sessions is 1.

```

user@PE1> show bgp group

```

```

Group Type: Internal AS: 65020 Local AS: 65020
Name: core-ibgp Index: 1 Flags: Export Eval
Holdtime: 0
Total peers: 1 Established: 1
192.168.10.1+179
bgp.l2vpn.0: 1/1/1/0
inter-as.l2vpn.0: 1/1/1/0

```

```

Groups: 1 Peers: 1 External: 0 Internal: 1 Down peers: 0 Flaps: 7
Table Tot Paths Act Paths Suppressed History Damp State Pending
bgp.l2vpn.0 1 1 0 0 0 0 0
inte.l2vpn.0 1 1 0 0 0 0 0

```

### Configuring the VPLS Routing Instances

#### Step-by-Step Procedure

To configure the VPLS routing instances:

1. On Router PE1, configure the VPLS routing instance. To enable a VPLS instance, specify the **vpls** instance type. Configure VPLS on the CE-facing Gigabit Ethernet interface. Configure the CE-facing interface to use **ethernet-vpls** encapsulation.

```

user@PE1# set routing-instances metro instance-type vpls
user@PE1# set routing-instances metro interface ge-1/3/0.0

```

2. On Router PE1, configure the VPLS protocol within the routing instance. To uniquely identify the virtual circuit, configure the VPLS identifier. The VPLS identifier uniquely identifies each VPLS in the router. Configure the same VPLS ID on all the routers for a given VPLS.

Specify the IP address of the **lo0** interface on Router ASBR2 as the neighbor.

Configure the CE-facing interface to use **ethernet-vpls** encapsulation and the **vpls** protocol family.

```

user@PE1# set routing-instances metro protocols vpls vpls-id 101
user@PE1# set routing-instances metro protocols vpls neighbor 192.168.3.1
user@PE1# set interfaces ge-1/3/0 encapsulation ethernet-vpls
user@PE1# set interfaces ge-1/3/0 unit 0 family vpls

```

3. On Router ASBR1, configure the VPLS routing instance. To enable a VPLS instance, specify the **vpls** instance type. Configure a route distinguisher and a VRF target. The **vrf-target** statement causes default VRF import and export policies to be generated that accept and tag routes with the specified target community.



**NOTE:** A route distinguisher allows the router to distinguish between two identical IP prefixes used as VPN routes. Configure a different route distinguisher on each ASBR router.



**NOTE:** You must configure the same VRF target on both ASBR routers.

```

user@ASBR1# set routing-instances inter-as instance-type vpls

```

```
user@ASBR1# set routing-instances inter-as route-distinguisher 65010:1
user@ASBR1# set routing-instances inter-as vrf-target target:2:1
```

4. On Router ASBR1, configure the VPLS protocol within the routing instance.

Configure the VPLS identifier. Specify the IP address of the lo0 interface on Router PE1 as the neighbor.

```
user@ASBR1# set routing-instances inter-as protocols vpls vpls-id 101
user@ASBR1# set routing-instances inter-as protocols vpls neighbor 192.168.2.1
```



**NOTE:** The VPLS identifier uniquely identifies each LDP-signaled VPLS in the router. Configure the same VPLS ID on Router PE1 and Router ASBR1.

5. On Router ASBR1, configure the VPLS site within the routing instance. Configure the site identifier as required by the protocol to establish the EBGp pseudowire. As a best practice for more complex topologies involving multihoming, configure a site preference.

```
user@ASBR1# set routing-instances inter-as protocols vpls site ASBR-metro
site-identifier 1
user@ASBR1# set routing-instances inter-as protocols vpls site ASBR-metro
site-preference 10000
```

6. On Router ASBR1, configure the VPLS mesh group **peer-as** statement within the routing instance to specify which ASs belong to this AS mesh group. Configure the peer AS for the mesh group as **all**.

This statement enables the router to establish a single pseudowire between the ASBR routers. VPLS NLRI messages are exchanged across the EBGp sessions on the inter-AS links between the ASBR routers. All autonomous systems are in one mesh group.

```
user@ASBR1# set routing-instances inter-as protocols vpls mesh-group metro
peer-as all
```

7. On ASBR2, configure the VPLS routing instance. To enable a VPLS instance, specify the **vpls** instance type. Configure a route distinguisher and a VRF target. The **vrf-target** statement causes default VRF import and export policies to be generated that accept and tag routes with the specified target community.



**NOTE:** A route distinguisher allows the router to distinguish between two identical IP prefixes used as VPN routes. Configure a different route distinguisher on each ASBR router.



**NOTE:** You must configure the same VRF target community on both ASBR routers.

```

user@ASBR2# set routing-instances inter-as instance-type vpls
user@ASBR2# set routing-instances inter-as route-distinguisher 65020:1
user@ASBR2# set routing-instances inter-as vrf-target target:2:1

```

8. On Router ASBR2, configure the VPLS site within the routing instance. Configure the site identifier as required by the protocol.

```

user@ASBR2# set routing-instances inter-as protocols vpls site ASBR-core
site-identifier 2

```

9. On Router ASBR2, configure the VPLS mesh group within the routing instance to specify which VPLS PEs belong to this AS mesh group. Configure the peer AS for the mesh group as **all**.

This statement enables the router to establish a single pseudowire between the ASBR routers. VPLS NLRI messages are exchanged across the EBGp sessions on the inter-AS links between the ASBR routers. All autonomous systems are in one mesh group.

```

user@ASBR1# set routing-instances inter-as protocols vpls mesh-group core peer-as
all

```

10. On Router PE2, configure the VPLS routing instance. To enable a VPLS instance, specify the **vpls** instance type. Configure VPLS on the CE-facing Gigabit Ethernet interface. Configure a route distinguisher and a VRF target.

```

user@PE2# set routing-instances inter-as instance-type vpls
user@PE2# set routing-instances inter-as interface ge-0/1/1.0
user@PE2# set routing-instances inter-as route-distinguisher 65020:1
user@PE2# set routing-instances inter-as vrf-target target:2:1

```

11. On Router PE2, configure the VPLS site within the routing instance. Configure the site identifier as required by the protocol.

Configure the CE-facing interface to use **ethernet-vpls** encapsulation and the **vpls** protocol family.

```

user@PE2# set routing-instances inter-as protocols vpls site PE2 site-identifier 3
user@PE2# set interfaces ge-0/1/1 encapsulation ethernet-vpls
user@PE2# set interfaces ge-0/1/1 unit 0 family vpls

```

12. On each router, commit the configuration:

```

user@host> commit check
configuration check succeeds
user@host> commit
commit complete

```

13. On the PE routers, display the CE-facing Gigabit Ethernet interface information and verify that the encapsulation is configured correctly:

```

user@host> show interfaces ge-1/3/0

```

| Address    | Interface  | Label space ID | Hold time |
|------------|------------|----------------|-----------|
| 10.0.23.10 | ge-1/3/1.0 | 192.168.3.1:0  | 11        |

Physical interface: ge-1/3/0, Enabled, Physical link is Up

Interface index: 147, SNMP ifIndex: 145

Link-level type: Ethernet, MTU: 1514, Speed: 1000Mbps, MAC-REWRITE Error: None,

Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled,

Auto-negotiation: Enabled, Remote fault: Online

Device flags : Present Running

Interface flags: SNMP-Traps Internal: 0x4000  
Link flags : None  
CoS queues : 4 supported, 4 maximum usable queues  
Schedulers : 256  
Current address: 00:12:1e:ee:34:db, Hardware address: 00:12:1e:ee:34:db  
Last flapped : 2008-08-27 19:02:52 PDT (5d 22:32 ago)  
Input rate : 0 bps (0 pps)  
Output rate : 0 bps (0 pps)  
Ingress rate at Packet Forwarding Engine : 0 bps (0 pps)  
Ingress drop rate at Packet Forwarding Engine : 0 bps (0 pps)  
Active alarms : None  
Active defects : None

Logical interface ge-1/3/0.0 (Index 84) (SNMP ifIndex 146)  
Flags: SNMP-Traps Encapsulation: ENET2  
Input packets : 0  
Output packets: 1  
Protocol inet, MTU: 1500  
Flags: None  
Addresses, Flags: Is-Preferred Is-Primary  
Destination: 10.10.11/24, Local: 10.10.11.11, Broadcast: 10.10.11.255

## Results

This section describes commands you can use to test the operation of the VPLS.

1. To verify the VPLS connections have been established, enter the **show vpls connections** command on Router PE1.

```
user@PE1> show vpls connections
Layer-2 VPN connections:
```

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -> -- only outbound connection is up           |
| CN -- circuit not provisioned    | <- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unknown connection status  | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not available              |
| BK -- Backup connection          | ST -- Standby connection                       |

Legend for interface status

Up -- operational  
Dn -- down

Instance: metro

VPLS-id: 101

| Neighbor                                                               | Type | St | Time last up        | # Up trans |
|------------------------------------------------------------------------|------|----|---------------------|------------|
| 192.168.3.1(vpls-id 101)                                               | rmt  | Up | Sep 9 14:05:18 2008 | 1          |
| Remote PE: 192.168.3.1, Negotiated control-word: No                    |      |    |                     |            |
| Incoming label: 800001, Outgoing label: 800000                         |      |    |                     |            |
| Local interface: vt-1/2/0.1048576, Status: Up, Encapsulation: ETHERNET |      |    |                     |            |
| Description: Intf - vpls metro neighbor 192.168.3.1 vpls-id 101        |      |    |                     |            |

In the display from Router PE1, verify that the neighbor is the **lo0** address of Router ASBR1 and that the status is **Up**.

2. To verify the VPLS connections have been established, enter the **show vpls connections** command on Router ASBR1.

```
user@ASBR1> show vpls connections
```

...

Instance: inter-as

BGP-VPLS State

Mesh-group connections: metro

| Neighbor                                                           | Local-site | Remote-site | St | Time last up        |
|--------------------------------------------------------------------|------------|-------------|----|---------------------|
| 192.168.10.1                                                       | 1          | 2           | Up | Sep 8 20:16:28 2008 |
| Incoming label: 800257, Outgoing label: 800000                     |            |             |    |                     |
| Local interface: vt-1/2/0.1049088, Status: Up, Encapsulation: VPLS |            |             |    |                     |

LDP-VPLS State

VPLS-id: 101

Mesh-group connections: \_\_ves\_\_

| Neighbor                                            | Type | St | Time last up        | # Up trans |
|-----------------------------------------------------|------|----|---------------------|------------|
| 192.168.2.1(vpls-id 101)                            | rmt  | Up | Sep 9 14:05:22 2008 | 1          |
| Remote PE: 192.168.2.1, Negotiated control-word: No |      |    |                     |            |

```

Incoming label: 800000, Outgoing label: 800001
Local interface: vt-0/1/0.1049089, Status: Up, Encapsulation: ETHERNET
Description: Intf - vpls inter-as neighbor 192.168.2.1 vpls-id 101

```

In the display from Router ASBR1, verify that the neighbor is the **lo0** address of Router PE1 and that the status is **Up**.

3. To verify the VPLS connections have been established, enter the **show vpls connections** command on Router ASBR2.

```

user@ASBR2> show vpls connections
...
Instance: inter-as
BGP-VPLS State
Mesh-group connections: __ves__
Neighbor Local-site Remote-site St Time last up
192.168.11.1 2 3 Up Sep 11 15:18:23 2008
Incoming label: 800002, Outgoing label: 800001
Local interface: vt-4/0/0.1048839, Status: Up, Encapsulation: VPLS
Mesh-group connections: core
Neighbor Local-site Remote-site St Time last up
192.168.3.1 2 1 Up Sep 8 20:16:28 2008
Incoming label: 800000, Outgoing label: 800257
Local interface: vt-4/0/0.1048834, Status: Up, Encapsulation: VPLS

```

In the display from Router ASBR2, verify that the neighbor is the **lo0** address of Router PE2 and that the status is **Up**.

4. To verify the VPLS connections have been established, enter the **show vpls connections** command on Router PE2.

```

user@PE2> show vpls connections
...
Instance: inter-as
Local site: PE2 (3)
connection-site Type St Time last up # Up trans
2 rmt Up Sep 8 20:16:28 2008 1
Remote PE: 192.168.10.1, Negotiated control-word: No
Incoming label: 800001, Outgoing label: 800002
Local interface: vt-0/3/0.1048832, Status: Up, Encapsulation: VPLS
Description: Intf - vpls inter-as local site 3 remote site 2

```

In the display from Router PE2, verify that the remote PE is the **lo0** address of Router ASBR2 and that the status is **Up**.

5. To verify that the CE routers can send and receive traffic across the VPLS, use the **ping** command.

```

user@CE1> ping 10.10.11.2
PING 10.10.11.2 (10.10.11.2): 56 data bytes
64 bytes from 10.10.11.2: icmp_seq=0 ttl=64 time=1.369 ms
64 bytes from 10.10.11.2: icmp_seq=1 ttl=64 time=1.360 ms
64 bytes from 10.10.11.2: icmp_seq=2 ttl=64 time=1.333 ms
^C

user@CE2> ping 10.10.11.1
PING 10.10.11.1 (10.10.11.1): 56 data bytes
64 bytes from 10.10.11.1: icmp_seq=0 ttl=64 time=6.209 ms
64 bytes from 10.10.11.1: icmp_seq=1 ttl=64 time=1.347 ms
64 bytes from 10.10.11.1: icmp_seq=2 ttl=64 time=1.324 ms
^C

```



If Router CE1 can send traffic to and receive traffic from Router CE2 and Router CE2 can send traffic to and receive traffic from Router CE1, the VPLS is performing correctly.

6. To display the configuration for Router CE1, use the **show configuration** command.

For your reference, the relevant sample configuration for Router CE1 follows.

```
interfaces {
 lo0 {
 unit 0 {
 family inet {
 address 192.168.1.1/32 {
 primary;
 }
 address 127.0.0.1/32;
 }
 }
 }
 ge-0/3/0 {
 unit 0 {
 family inet {
 address 10.10.11.1/24;
 }
 }
 }
}
```

7. To display the configuration for Router PE1, use the **show configuration** command.

For your reference, the relevant sample configuration for Router PE1 follows.

```
interfaces {
 lo0 {
 unit 0 {
 family inet {
 address 192.168.2.1/32 {
 primary;
 }
 address 127.0.0.1/32;
 }
 }
 }
 ge-1/3/0 {
 encapsulation ethernet-vpls;
 unit 0 {
 family vpls;
 }
 }
 ge-1/3/1 {
 unit 0 {
 family inet {
 address 10.0.23.9/30;
 }
 family mpls;
 }
 }
}
```

```

routing-options {
 autonomous-system 0.65010;
}
protocols {
 mpls {
 interface ge-1/3/1.0;
 }
 ospf {
 traffic-engineering;
 area 0.0.0.1 {
 interface ge-1/3/1.0;
 interface lo0.0 {
 passive;
 }
 }
 }
 ldp {
 interface ge-1/3/1.0;
 interface lo0.0;
 }
}
routing-instances {
 metro {
 instance-type vpls;
 interface ge-1/3/0.0;
 protocols {
 vpls {
 vpls-id 101;
 neighbor 192.168.3.1;
 }
 }
 }
}

```

8. To display the configuration for Router ASBR1, use the **show configuration** command.

For your reference, the relevant sample configuration for Router ASBR1 follows.

```

interfaces {
 lo0 {
 unit 0 {
 family inet {
 address 192.168.3.1/32 {
 primary;
 }
 address 127.0.0.1/32;
 }
 }
 }
 ge-0/3/0 {
 unit 0 {
 family inet {
 address 10.0.78.1/30;
 }
 family mpls;
 }
 }
}

```

```

ge-0/3/1 {
 unit 0 {
 family inet {
 address 10.0.23.10/30;
 }
 family mpls;
 }
}
routing-options {
 autonomous-system 0.65010;
}
protocols {
 mpls {
 interface ge-0/3/1.0;
 interface ge-0/3/0.0;
 }
 bgp {
 group vpls-core {
 type external;
 multihop;
 local-address 192.168.3.1;
 family l2vpn {
 signaling;
 }
 peer-as 65020;
 neighbor 192.168.10.1;
 }
 group metro-core {
 type external;
 local-address 10.0.78.1;
 family inet {
 labeled-unicast {
 resolve-vpn;
 }
 }
 export loopback;
 peer-as 65020;
 neighbor 10.0.78.2;
 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.1 {
 interface ge-0/3/1.0;
 interface lo0.0 {
 passive;
 }
 }
 }
 ldp {
 interface ge-0/3/0.0;
 interface ge-0/3/1.0;
 interface lo0.0;
 }
}

```

```

policy-options {
 policy-statement loopback {
 term term1 {
 from {
 protocol [ospf direct];
 route-filter 192.168.0.0/16 longer;
 }
 then accept;
 }
 }
}
routing-instances {
 inter-as {
 instance-type vpls;
 route-distinguisher 65010:1;
 vrf-target target:2:1;
 protocols {
 vpls {
 site ASBR-metro {
 site-identifier 1;
 site-preference 10000;
 }
 vpls-id 101;
 neighbor 192.168.2.1;
 mesh-group metro {
 peer-as {
 all;
 }
 }
 }
 }
 }
}

```

9. To display the configuration for Router ASBR2, use the **show configuration** command.

For your reference, the relevant sample configuration for Router ASBR2 follows.

```

interfaces {
 lo0 {
 unit 0 {
 family inet {
 address 192.168.10.1/32 {
 primary;
 }
 address 127.0.0.1/32;
 }
 }
 }
 ge-3/1/0 {
 unit 0 {
 family inet {
 address 10.0.78.2/30;
 }
 family mpls;
 }
 }
}

```

```

ge-3/1/1 {
 unit 0 {
 family inet {
 address 10.0.90.13/30;
 }
 family mpls;
 }
}
routing-options {
 autonomous-system 0.65020;
}
protocols {
 mpls {
 interface ge-3/1/0.0;
 interface ge-3/1/1.0;
 }
 bgp {
 group core-ibgp {
 type internal;
 local-address 192.168.10.1;
 family inet {
 labeled-unicast {
 resolve-vpn;
 }
 }
 family l2vpn {
 signaling;
 }
 neighbor 192.168.11.1;
 }
 group vpls-metro {
 type external;
 multihop;
 local-address 192.168.10.1;
 family l2vpn {
 signaling;
 }
 peer-as 65010;
 neighbor 192.168.3.1;
 }
 group core-metro {
 type external;
 local-address 10.0.78.2;
 family inet {
 labeled-unicast {
 resolve-vpn;
 }
 }
 export loopback;
 peer-as 65010;
 neighbor 10.0.78.1;
 }
 }
 ospf {
 traffic-engineering;
 }
}

```

```

 area 0.0.0.0 {
 interface ge-3/1/1.0;
 interface lo0.0 {
 passive;
 }
 }
 }
 ldp {
 interface ge-3/1/0.0;
 interface ge-3/1/1.0;
 }
}
policy-options {
 policy-statement loopback {
 term term1 {
 from {
 protocol [ospf direct];
 route-filter 192.168.0.0/16 longer;
 }
 then accept;
 }
 }
}
routing-instances {
 inter-as {
 instance-type vpls;
 route-distinguisher 65020:1;
 vrf-target target:2:1;
 protocols {
 vpls {
 site ASBR-core {
 site-identifier 2;
 }
 mesh-group core {
 peer-as {
 all;
 }
 }
 }
 }
 }
}
}

```

10. To display the configuration for Router PE2, use the **show configuration** command.

For your reference, the relevant sample configuration for Router PE2 follows.

```

interfaces {
 lo0 {
 unit 0 {
 family inet {
 address 192.168.11.1/32 {
 primary;
 }
 address 127.0.0.1/32;
 }
 }
 }
}

```

```

}
ge-0/1/0 {
 unit 0 {
 family inet {
 address 10.0.90.14/30;
 }
 family mpls;
 }
}
ge-0/1/1 {
 encapsulation ethernet-vpls;
 unit 0 {
 family vpls;
 }
}
}
routing-options {
 autonomous-system 0.65020;
}
protocols {
 mpls {
 interface ge-0/1/0.0;
 }
 bgp {
 group core-ibgp {
 type internal;
 local-address 192.168.11.1;
 family l2vpn {
 signaling;
 }
 neighbor 192.168.10.1;
 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface ge-0/1/0.0;
 interface lo0.0 {
 passive;
 }
 }
 }
 ldp {
 interface ge-0/1/0.0;
 }
}
routing-instances {
 inter-as {
 instance-type vpls;
 interface ge-0/1/1.0;
 route-distinguisher 65020:1;
 vrf-target target:2:1;
 protocols {
 vpls {
 site PE2 {
 site-identifier 3;
 }
 }
 }
 }
}

```

```
 }
 }
}
}
```

11. To display the configuration for Router CE2, use the **show configuration** command.

For your reference, the relevant sample configuration for Router CE2 follows.

```
interfaces {
 lo0 {
 unit 0 {
 family inet {
 address 192.168.12.1/32 {
 primary;
 }
 address 127.0.0.1/32;
 }
 }
 }
 ge-0/1/1 {
 unit 0 {
 family inet {
 address 10.10.11.2/24;
 }
 }
 }
}
```

**Related  
Documentation**

---

## Configuring VPLS and Integrated Routing and Bridging

Traditional Layer 2 switching environments consist of Layer 2 devices (such as switches) that partition data into broadcast domains. The broadcast domains can be created through physical topologies or logically through virtual local area networks (VLANs). For MX Series routers, you can logically configure broadcast domains within virtual switch routing instances, VPLS routing instances, or bridging domains. The individual routing instances or bridging domains are differentiated through VLAN identifiers and these instances or domains function much like traditional VLANs.

To configure a VLAN with IRB support, include the following statements:

```
[edit]
routing-instances {
 instance-name {
 instance-type vpls;
 vlan-id (VLAN) id;
 route-distinguisher distinguisher;
 vrf-target target;
 interface interface-name;
 interface interface-name;
 routing-interface interface-name;
```



```
}
}
```

In multihomed VPLS configurations, you can configure VPLS to keep a VPLS connection up if only an IRB interface is available by configuring the **irb** option for the **connectivity-type** statement at the **[edit routing-instances routing-instance-name protocols vpls]** hierarchy level. The **connectivity-type** statement has the **ce** and **irb** options. The **ce** option is the default and specifies that a CE interface is required to maintain the VPLS connection. By default, if only an IRB interface is available, the VPLS connection is brought down.



**NOTE:** A maximum of 4096 active logical interfaces are supported for a VLAN or on each mesh group in a VPLS routing instance configured for Layer 2 bridging.

For detailed information and configuration instructions on bridging domains and spanning tree protocol, see the *Junos OS Network Interfaces Library for Routing Devices* and *Junos OS Routing Protocols Library*.

The following sections provide configuration information specific to VPLS in regards to integrated routing and bridging:

- [Configuring MAC Address Flooding and Learning for VPLS on page 893](#)
- [Configuring MSTP for VPLS on page 894](#)

## Configuring MAC Address Flooding and Learning for VPLS

In a VPLS routing instance or bridge domain, when a frame is received from a CE interface, it is flooded to the other CE interfaces and all of the VE interfaces if the destination MAC address is not learned or if the frame is either broadcast or multicast. If the destination MAC address is learned on another CE device, such a frame is unicast to the CE interface on which the MAC address is learned. This might not be desirable if the service provider does not want CE devices to communicate with each other directly.

To prevent CE devices from communicating directly include the **no-local-switching** statement at the **[edit bridge-domains bridge-domain-name]** hierarchy level:

```
[edit bridge-domains bridge-domain-name]
no-local-switching;
```

The **no-local-switching** statement is available only on MX Series routers. If you include it, frames arriving on a CE interface are sent to VE or core-facing interfaces only.



**NOTE:** (MX80, MX104, and the 16x10GE MPC, MPC1, or MPC2 on MX240, MX480, MX960, MX2010, and MX2020 only) If you configure the **no-local-switching** command at the **[edit bridge-domains bridge-domain-name]** hierarchy level, it might not prevent multicast traffic from being forwarded between the CE-facing interfaces of the bridge domain. Broadcast, unknown unicast, and known multicast traffic does not exhibit this behavior.

## Configuring MSTP for VPLS

When you configure integrated routing and bridging, you might also need to configure the Multiple Spanning Tree Protocol (MSTP). When you configure MSTP on a provider edge (PE) router running VPLS, you must also configure **ethernet-vpls** encapsulation on the customer-facing interfaces. VLAN-based VPLS interface encapsulations are not supported with MSTP.

### Related Documentation

- *Configuring Integrated Routing and Bridging for VLANs*
- *Configuring Integrated Routing and Bridging in a VPLS Instance (MX Series Routers Only)*
- [Example: Configuring Inter-AS VPLS with MAC Processing at the ASBR on page 867](#)
- *Example: VPLS Configuration (BGP and LDP Interworking)*
- *Example: VPLS Configuration (BGP Signaling)*

# Configuring Load Balancing and Performance

- [Configuring VPLS Load Balancing on page 895](#)
- [Configuring VPLS Load Balancing Based on IP and MPLS Information on page 897](#)
- [Configuring VPLS Load Balancing on MX Series 3D Universal Edge Routers on page 898](#)
- [MAC Moves Loop Prevention in VPLS Network Overview on page 900](#)
- [Configuring VPLS Loop Prevention Due to MAC Moves on page 901](#)
- [Example: Configuring Loop Prevention in VPLS Network Due to MAC Moves on page 903](#)
- [Configuring Improved VPLS MAC Address Learning on T4000 Routers with Type 5 FPCs on page 918](#)

## Configuring VPLS Load Balancing

---

By default, when there are multiple equal-cost paths to the same destination for the active route, the Junos OS uses a hash algorithm to select one of the next-hop addresses to install in the forwarding table. Whenever the set of next hops for a destination changes, the next-hop address is reselected using the hash algorithm.

You can configure the Junos OS so that, for the active route, all next-hop addresses for a destination are installed in the forwarding table. This feature is called per-packet load balancing. You can use load balancing to spread traffic across multiple paths between routers. You can also configure per-packet load balancing to optimize VPLS traffic flows across multiple paths.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

You can load-balance VPLS traffic based on Layer 2 media access control (MAC) information, IP information and MPLS labels, or MPLS labels only.



**NOTE:** For platform support information, see [family multiservice](#).

To optimize VPLS traffic flows across multiple paths, include the **family multiservice** statement at the **[edit forwarding-options hash-key]** hierarchy level:

```
family multiservice {
 destination-mac;
 label-1;
 label-2;
 payload {
 ip {
 layer-3 {
 (destination-ip-only | source-ip-only);
 }
 layer-3-only;
 layer-4;
 }
 }
 source-mac;
 symetric-hash {
 complement;
 }
}
```

You can configure one or more of the following options to load-balance using the specified packet information:

- **destination-mac**—Include the destination-address MAC information in the hash key for Layer 2 load balancing.
- **source-mac**—Include the source-address MAC information in the hash key.
- **label-1**—Include the first MPLS label in the hash key. Used for including a one-label packet for per-flow load balancing of IPv4 VPLS traffic based on IP information and MPLS labels.
- **label-2**—Include the second MPLS label in the hash key. If both **label-1** and **label-2** are specified, the entire first label and the first 16 bits of the second label are hashed.
- **payload**—Include the packet's IP payload in the hash key.
- **ip**—Include the IP address of the IPv4 or IPv6 payload in the hash key.
- **layer-3-only**—Include only the Layer 3 information from the packet's IP payload in the hash key.
- **layer-3**—Include Layer 3 information from the packet's IP payload in the hash key.
- **destination-address-only**—Include only the destination IP address in the payload in the hash key.



**NOTE:** You can include either the **source-address-only** or the **destination-address-only** statement, not both. They are mutually exclusive.

- **source-address-only**—Include only the source IP address in the payload in the hash key.



**NOTE:** You can include either the `source-address-only` or the `destination-address-only` statement, not both. They are mutually exclusive.

- **layer-4**—Include Layer 4 information from the packet's IP payload in the hash key.
- **symmetric-hash**—Configure the symmetric hash or symmetric hash complement for configuring symmetrical load balancing on an 802.3ad Link Aggregation Group.
- **complement**—Include the complement of the symmetric hash in the hash key.

For more information about how to configure per-packet load balancing, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*.

**Related Documentation**

- [Configuring VPLS Load Balancing Based on IP and MPLS Information on page 897](#)
- [Configuring VPLS Load Balancing on MX Series 3D Universal Edge Routers on page 898](#)

## Configuring VPLS Load Balancing Based on IP and MPLS Information

In Junos OS Release 9.4 and later, you can configure load balancing for VPLS traffic to have the hash key include IP information and MPLS labels on the M120 and M320 routers only. In earlier Junos OS Releases, you can configure load balancing based only on Layer 2 information. In Junos OS Release 9.5 and later, you can configure load balancing for VPLS traffic based on Layer 3 IP and Layer 4 information on MX Series routers only. For more information, see “[Configuring VPLS Load Balancing on MX Series 3D Universal Edge Routers](#)” on page 898.

For IPv4 traffic, only the IP source and destination addresses are included in the hash key. For MPLS and IPv4 traffic, one or two MPLS labels and IPv4 source and destination addresses are included. For MPLS Ethernet pseudowires, only one or two MPLS labels are included in the hash key.



**NOTE:** VPLS load balancing based on MPLS labels and IP information is supported only on the M120 and M320 routers. In Junos OS Release 9.5 and later, on MX Series routers only, you can configure VPLS load balancing based on IP and Layer 4 information.

To optimize VPLS flows across multiple paths based on IP and MPLS information, include the `family multiservice` statement at the `[edit forwarding-options hash-key]` hierarchy level:

```
[edit forwarding-options hash-key]
family multiservice {
 label-1;
 label-2;
 payload {
 ip {
 layer-3-only;
 }
 }
}
```

```
}
}
```

To use the first MPLS label in the hash key, include the **label-1** statement:

```
[edit forwarding-options hash-key family multiservice]
label-1;
```

To use the second MPLS label, include both the **label-1** and **label-2** statements:

```
[edit forwarding-options hash-key family multiservice]
label-1;
label-2;
```

To use the packet's IPv4 payload in the hash key, include the **payload** and **ip** statements:

```
[edit forwarding-options hash-key family multiservice]
payload {
 ip;
}
```



**NOTE:** Only IPv4 is supported.

To include only Layer 3 information from the IPv4 payload, specify the **layer-3-only** option to the **payload ip** statement:

```
[edit forwarding-options hash-key family multiservice]
payload {
 ip {
 layer-3-only;
 }
}
```

To use the first and second MPLS labels and the packet's IP payload in the hash key, include the **label-1**, **label-2**, and **payload ip** statements:

```
[edit forwarding-options hash-key family multiservice]
label-1;
label-2;
payload {
 ip;
}
```

---

## Configuring VPLS Load Balancing on MX Series 3D Universal Edge Routers

In Junos OS Release 9.5 and later, on MX Series routers, you can configure the load balancing hash key for Layer 2 traffic to use fields in the Layer 3 and Layer 4 headers inside the frame payload. You can also configure VPLS load balancing based on IP and MPLS information on M120 and M320 routers only. For more information, see [“Configuring VPLS Load Balancing Based on IP and MPLS Information” on page 897](#).

You can configure load balancing on MX Series routers based on Layer 3 or Layer 4 information or both.

To configure VPLS load balancing on the MX Series router to include either Layer 3 IP information or Layer 4 headers or both:

1. Include the **payload** statement at the **[edit forwarding-options hash-key family multiservice]** hierarchy level.
2. Include the **ip** statement at the **[edit forwarding-options hash-key family multiservice payload]** hierarchy level.

To configure VPLS load balancing to include the Layer 3 information:

1. Include the **layer-3** statement at the **[edit forwarding-options hash-key family multiservice payload ip]** hierarchy level.
2. Include the **source-ip-only** statement at the **[edit forwarding-options hash-key family multiservice payload ip layer-3]** hierarchy level to include information about the IP source address only in the hash key.
3. Include **destination-ip-only** statement at the **[edit forwarding-options hash-key family multiservice payload ip layer-3]** hierarchy level to include information about the IP destination address only in the hash key.



**NOTE:** You can configure either the **source-ip-only** or the **destination-ip-only** statements at a time, not both. They are mutually exclusive.

To configure VPLS load balancing to include Layer 4 information:

- Include the **layer-4** statement at the **[edit forwarding-options hash-key family multiservice payload ip]** hierarchy level.

The following example shows load balancing configured to use the source Layer 3 IP address option and Layer 4 header fields as well as the source and destination MAC addresses:

```
[edit forwarding-options hash-key]
family multiservice {
 source-mac;
 destination-mac;
 payload {
 ip {
 layer-3 {
 source-ip-only;
 }
 layer-4;
 }
 }
}
```

- Related Documentation**
- [family multiservice on page 1109](#)
  - *hash-key*

## MAC Moves Loop Prevention in VPLS Network Overview

---

In a virtual private LAN service (VPLS) deployment, when a previously learned media access control (MAC) address appears on a different physical interface, for example, local interfaces (Gigabit Ethernet interfaces) or label switched Interfaces (LSIs), or within a different unit of the same physical interface and if this behavior occurs frequently, then it is considered a MAC move.

You can configure the router to report a MAC address move based on the following parameters:

- Number of times a MAC address move occurs
- Specified period of time over which the MAC address move occurs

Configuration errors at the network can force traffic into never ending circular paths or loops. These loops in the VPLS network cause frequent MAC moves between different interfaces which can be used to rectify the problem by disabling such an interface in the network. The following two approaches can be used to disable the interface causing the loop:

- Base learning interface (base IFL) approach algorithm- This is the primary approach used to disable the looped interface. Base interface information is maintained for every MAC in the routing instance. If the MAC stays at the interface it was first learned for 300 seconds, then the interface-MAC association is considered to be stable and this interface is considered as the base interface of the MAC. If the MAC move happens frequently between the local interface and the LSI interface while the base interface of the MAC is an LSI, then the local interface is considered to be looped and has to be disabled.
- Statistical approach algorithm- This is the secondary approach used to disable the looped interface. If the MAC has not been learned for over 300 seconds at an interface, then it does not have a base interface and hence the statistical approach is used.

If the MAC that has no base interface information( Base Learning interface is null) starts moving, then the statistics of such MAC moves between different interfaces is learned. If the statistics show MAC moves from LSI to local interface or from local interface to local interface, then the local interface is considered to be looped and is disabled.

There are certain MACs that can move between different interfaces, for example, mastership change in the Virtual Router Redundancy Protocol (VRRP). The base interface of such MAC moves cannot be maintained as this leads to the assumption of a loop creation. Hence, such MACs should be configured as virtual MACs. Example of virtual MACs are 00:00:5e:00:01:xx for VRRP, 00:00:0c:07:ac:xx for hot standby router protocol (HSRP) , 00:07:b4:00:01:xx for global server load balancing (GSLB), and 02:bf:xx:xx:xx:xx for VMotion.

The following timers help in monitoring the disabled interfaces:



- **Cooloff time** — The cooloff time starts when the interface gets disabled. During this time any MAC move happening in the routing instance is ignored. This ensures that only one interface is blocked at a given time on a routing instance, and blocking of another interface happens only after the expiration of the cooloff timer provided the given MAC moves are still observed. By default, the cooloff time is 30 seconds.
- **Interface recovery time** — When an interface gets disabled, it is disabled permanently. Configuring the interface recovery time ensures that the interface gets enabled on completion of the interface recovery time duration.
- **Statistical approach wait time** — The time when the statistics are collected after MAC moves are observed to determine the existence of a loop when there is no base IFL for the MAC address. . By default, the statistical approach wait timer is 30 seconds.

**Related Documentation**

- [Example: Configuring Loop Prevention in VPLS Network Due to MAC Moves on page 904](#)
- [virtual-mac on page 1223](#)
- [vpls-mac-move on page 1231](#)

## Configuring VPLS Loop Prevention Due to MAC Moves

In a virtual private LAN service (VPLS) deployment, when a previously learned media access control (MAC) address appears on a different physical interface, for example, local interfaces (Gigabit Ethernet interfaces) or label switched Interfaces (LSIs), or within a different unit of the same physical interface and if this behavior occurs frequently, then it is considered a MAC move. The router reports a MAC address move based on the number of times a MAC address move occurs and the specified period of time over which the MAC address move occurs. Configuration errors at the VPLS network can lead to loops that cause frequent MAC moves between different interfaces. These moves can be used to rectify the problem by disabling such interface in the network. The following two approaches can be used to disable the interface:

- **Base learning interface (base IFL) approach algorithm**— This is the primary approach used to disable the looped local interface.
- **Statistical approach algorithm** — This is the secondary approach used to disable the looped local interface.

Some virtual MACs can genuinely move between different interfaces and such MACs can be configured to ignore the moves. The cooloff time and the statistical approach wait time are used internally to find out the looped interface. The interface recovery time can be configured to auto-enable the interface that gets disabled due to a loop in the network.

Before you begin to configure loop prevention in a VPLS network:

1. Configure the VPLS topology.
2. Configure the VPLS routing instances.

3. Enable VPLS MAC move action on a VPLS instance.
4. Configure the routing and signaling protocols.

To configure loop prevention in a VPLS network:

1. Configure the threshold time and the threshold count to detect MAC moves.

```
[edit protocols l2-learning global-mac-move]
user@host# set threshold-time seconds
user@host# set threshold-count seconds
```

For example, configure the threshold time as 30 and the threshold count as 4 to detect MAC moves.

```
[edit protocols l2-learning global-mac-move]
user@host# set threshold-time 30
user@host# set threshold-count 4
```



**NOTE:** If the threshold time and threshold count are not configured, then the default values are used. The default value of threshold time is 1 second, and default value of threshold count is 50.

2. (Optional) Configure a cooloff time to ensure that no other interface gets disabled once an interface, for a routing instance, is disabled during this time period.

```
[edit protocols l2-learning vpls-mac-move]
user@host# set cooloff-time seconds
```

3. (Optional) Configure the statistical approach wait time to determine the existence of a loop based on the statistics collected after MAC moves are observed when there is no base IFL for the MAC address.

```
[edit protocols l2-learning vpls-mac-move]
user@host# set statistical-approach-wait-time seconds
```

4. (Optional) Configure the interface recovery time to ensure that the disabled interface gets enabled on completion of the interface recovery time duration.

```
[edit protocols l2-learning vpls-mac-move]
user@host# set interface-recovery-time seconds
```

5. (Optional) Configure the virtual MAC address to ignore the MAC moves as this leads to the assumption of loop creation.

```
[edit protocols l2-learning vpls-mac-move]
user@host# set virtual-mac mac-address
```

6. Configure the VPLS routing instance of an interface.

```
[edit routing-instances instance-name]
user@host# set instance-type vpls
user@host# set interface interface
```

7. Enable MAC move action on the interface for the VPLS instance, and configure the VPLS neighbor.

```
[edit routing-instances instance-name]
```

```

user@host# set protocols vpls enable-mac-move-action
user@host# set protocols vpls no-tunnel-services
user@host# set protocols vpls vpls-id vpls-id
user@host# set protocols vpls neighbor IP-address

```

- Related Documentation**
- [Example: Configuring Loop Prevention in VPLS Network Due to MAC Moves on page 903](#)
  - [MAC Moves Loop Prevention in VPLS Network Overview on page 900](#)

## Example: Configuring Loop Prevention in VPLS Network Due to MAC Moves

- [MAC Moves Loop Prevention in VPLS Network Overview on page 903](#)
- [Example: Configuring Loop Prevention in VPLS Network Due to MAC Moves on page 904](#)

### MAC Moves Loop Prevention in VPLS Network Overview

In a virtual private LAN service (VPLS) deployment, when a previously learned media access control (MAC) address appears on a different physical interface, for example, local interfaces (Gigabit Ethernet interfaces) or label switched Interfaces (LSIs), or within a different unit of the same physical interface and if this behavior occurs frequently, then it is considered a MAC move.

You can configure the router to report a MAC address move based on the following parameters:

- Number of times a MAC address move occurs
- Specified period of time over which the MAC address move occurs

Configuration errors at the network can force traffic into never ending circular paths or loops. These loops in the VPLS network cause frequent MAC moves between different interfaces which can be used to rectify the problem by disabling such an interface in the network. The following two approaches can be used to disable the interface causing the loop:

- Base learning interface (base IFL) approach algorithm– This is the primary approach used to disable the looped interface. Base interface information is maintained for every MAC in the routing instance. If the MAC stays at the interface it was first learned for 300 seconds, then the interface-MAC association is considered to be stable and this interface is considered as the base interface of the MAC. If the MAC move happens frequently between the local interface and the LSI interface while the base interface of the MAC is an LSI, then the local interface is considered to be looped and has to be disabled.
- Statistical approach algorithm– This is the secondary approach used to disable the looped interface. If the MAC has not been learned for over 300 seconds at an interface, then it does not have a base interface and hence the statistical approach is used.

If the MAC that has no base interface information( Base Learning interface is null) starts moving, then the statistics of such MAC moves between different interfaces is learned. If the statistics show MAC moves from LSI to local interface or from local

interface to local interface, then the local interface is considered to be looped and is disabled.

There are certain MACs that can move between different interfaces, for example, mastership change in the Virtual Router Redundancy Protocol (VRRP). The base interface of such MAC moves cannot be maintained as this leads to the assumption of a loop creation. Hence, such MACs should be configured as virtual MACs. Example of virtual MACs are 00:00:5e:00:01:xx for VRRP, 00:00:0c:07:ac:xx for hot standby router protocol (HSRP), 00:07:b4:00:01:xx for global server load balancing (GSLB), and 02:bf:xx:xx:xx:xx for VMotion.

The following timers help in monitoring the disabled interfaces:

- **Cooloff time** — The cooloff time starts when the interface gets disabled. During this time any MAC move happening in the routing instance is ignored. This ensures that only one interface is blocked at a given time on a routing instance, and blocking of another interface happens only after the expiration of the cooloff timer provided the given MAC moves are still observed. By default, the cooloff time is 30 seconds.
- **Interface recovery time** — When an interface gets disabled, it is disabled permanently. Configuring the interface recovery time ensures that the interface gets enabled on completion of the interface recovery time duration.
- **Statistical approach wait time** — The time when the statistics are collected after MAC moves are observed to determine the existence of a loop when there is no base IFL for the MAC address. By default, the statistical approach wait timer is 30 seconds.

### Example: Configuring Loop Prevention in VPLS Network Due to MAC Moves

This example shows how to prevent a loop in the VPLS network due to MAC moves between different physical interfaces.

When a MAC move is detected in the VPLS network, Junos OS allows the prevention of the loop in the network by disabling the interface using a base IFL or statistical approach algorithm.

- [Requirements on page 904](#)
- [Overview on page 905](#)
- [Configuration on page 906](#)
- [Verification on page 913](#)

---

#### Requirements

This example uses the following hardware and software components:

- Four MX Series 3D Universal Edge Routers
- Junos OS Release 14.2 or later running on all devices

Before you begin:

1. Configure the VPLS topology.
2. Configure the VPLS routing instances.
3. Enable VPLS MAC move action on a VPLS instance.
4. Configure the routing and signaling protocols.

### Overview

---

Starting with Junos OS Release 14.2, the loop creation in the VPLS network due to frequent MAC moves between different physical interfaces can be prevented by identifying and disabling such interfaces using the base IFL approach or statistical approach algorithm.

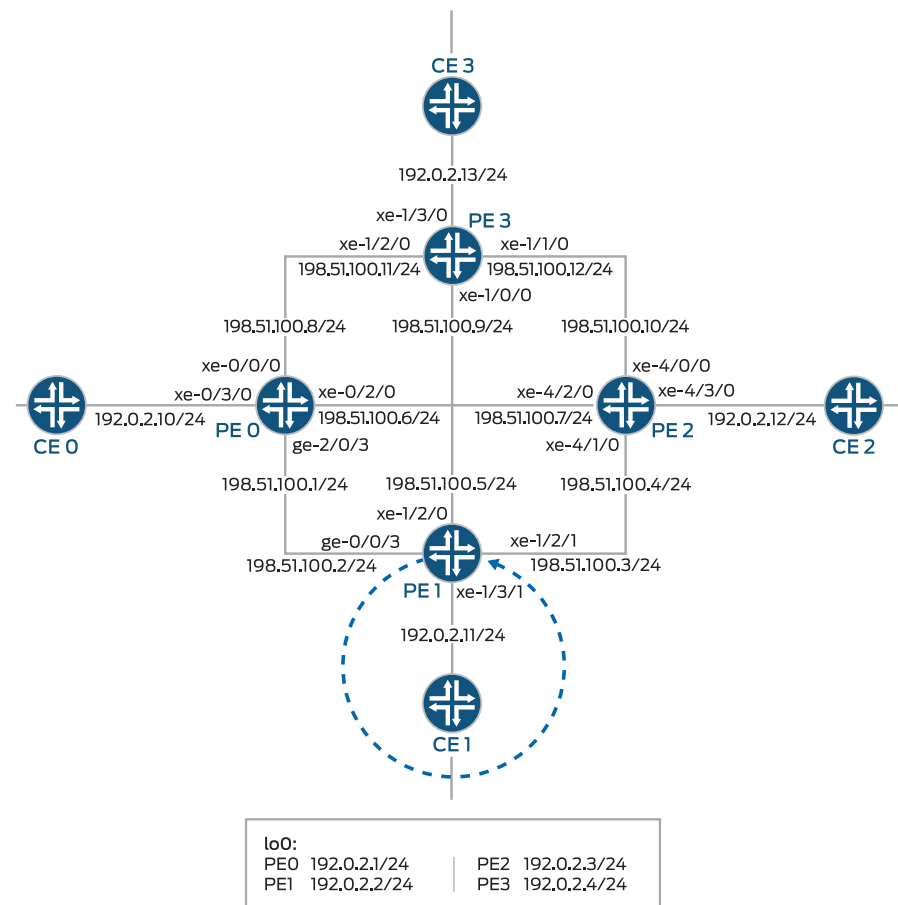
The *base IFL approach* algorithm is the primary approach. Base interface information is maintained for every MAC in the routing instance. If the MAC stays at the interface it was first learned for 300 seconds, then the interface-MAC association is considered to be stable, and this interface is considered as the base interface of the MAC. If the MAC move happens frequently between the local interface and the LSI interface while the base interface of the MAC is an LSI, then the local interface is considered to be looped and has to be disabled.

The *statistical approach* algorithm is the secondary approach used to disable the looped interface. If the MAC has not been learned for over 300 seconds at an interface, then it does not have a base interface and hence the statistical approach is used. If the MAC that has no base interface information (Base Learning interface is null) starts moving then the statistics of such MAC moves between different interfaces is learned. If the statistics show MAC moves from LSI to local interface or from local interface to local interface then the local interface is considered to be looped and is disabled.

### Topology

In the topology shown in [Figure 80 on page 906](#), a loop was detected on Device PE1 in the VPLS network.

Figure 80: Example Loop Prevention Due to MAC Move in VPLS Network



g042468

### 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.

```

PE0
set interfaces xe-0/0/0 unit 0 family inet address 198.51.100.5/24
set interfaces xe-0/0/0 unit 0 family mpls
set interfaces xe-0/2/0 unit 0 family inet address 198.51.100.6/24
set interfaces xe-0/2/0 unit 0 family mpls
set interfaces xe-0/3/0 vlan-tagging
set interfaces xe-0/3/0 encapsulation vlan-vpls
set interfaces xe-0/3/0 unit 600 encapsulation vlan-vpls
set interfaces xe-0/3/0 unit 600 vlan-id 600
set interfaces ge-2/0/3 unit 0 family inet address 198.51.100.1/24
set interfaces ge-2/0/3 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 192.0.2.1/24

```

```

set routing-options router-id 192.0.2.1
set routing-options autonomous-system 701
set protocols mpls interface fxp0.0 disable
set protocols mpls interface ge-2/0/3.0
set protocols mpls interface xe-0/2/0.0
set protocols mpls interface xe-0/0/0.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface ge-2/0/3.0 interface-type p2p
set protocols ospf area 0.0.0.0 interface ge-2/0/3.0 metric 10
set protocols ospf area 0.0.0.0 interface xe-0/2/0.0 interface-type p2p
set protocols ospf area 0.0.0.0 interface xe-0/2/0.0 metric 10
set protocols ospf area 0.0.0.0 interface xe-0/0/0.0 interface-type p2p
set protocols ospf area 0.0.0.0 interface xe-0/0/0.0 metric 10
set protocols ldp interface xe-0/0/0.0
set protocols ldp interface xe-0/2/0.0
set protocols ldp interface ge-2/0/3.0
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0
set protocols l2-learning global-mac-move threshold-time 30
set protocols l2-learning global-mac-move threshold-count 4
set protocols l2-learning vpls-mac-move cooloff-time 10
set protocols l2-learning vpls-mac-move statistical-approach-wait-time 10
set protocols l2-learning vpls-mac-move interface-recovery-time 5
set protocols l2-learning vpls-mac-move virtual-mac 00:00:5e:00:01:00/40
set routing-instances vpls_1 instance-type vpls
set routing-instances vpls_1 interface xe-0/3/0.600
set routing-instances vpls_1 protocols vpls no-tunnel-services
set routing-instances vpls_1 protocols vpls vpls-id 100
set routing-instances vpls_1 protocols vpls neighbor 192.0.2.2
set routing-instances vpls_1 protocols vpls neighbor 192.0.2.3
set routing-instances vpls_1 protocols vpls neighbor 192.0.2.4

```

```

PE1 set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.2/24
set interfaces ge-0/0/3 unit 0 family mpls
set interfaces xe-1/2/0 unit 0 family inet address 198.51.100.5/24
set interfaces xe-1/2/0 unit 0 family mpls
set interfaces xe-1/2/1 unit 0 family inet address 198.51.100.3/24
set interfaces xe-1/2/1 unit 0 family mpls
set interfaces xe-1/3/1 vlan-tagging
set interfaces xe-1/3/1 encapsulation vlan-vpls
set interfaces xe-1/3/1 unit 600 encapsulation vlan-vpls
set interfaces xe-1/3/1 unit 600 vlan-id 600
set interfaces lo0 unit 0 family inet address 192.0.2.2/24
set routing-options router-id 192.0.2.2
set routing-options autonomous-system 701
set protocols mpls interface fxp0.0 disable
set protocols mpls interface ge-0/0/3.0
set protocols mpls interface xe-1/2/1.0
set protocols mpls interface xe-1/2/0.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface ge-0/0/3.0 interface-type p2p
set protocols ospf area 0.0.0.0 interface ge-0/0/3.0 metric 10
set protocols ospf area 0.0.0.0 interface xe-1/2/1.0 interface-type p2p
set protocols ospf area 0.0.0.0 interface xe-1/2/1.0 metric 10

```

```

set protocols ospf area 0.0.0.0 interface xe-1/2/0.0 interface-type p2p
set protocols ospf area 0.0.0.0 interface xe-1/2/0.0 metric 10
set protocols ldp interface ge-0/0/3.0
set protocols ldp interface xe-1/2/0.0
set protocols ldp interface xe-1/2/1.0
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0
set protocols l2-learning global-mac-move threshold-time 30
set protocols l2-learning global-mac-move threshold-count 4
set protocols l2-learning vpls-mac-move cooloff-time 10
set protocols l2-learning vpls-mac-move statistical-approach-wait-time 10
set protocols l2-learning vpls-mac-move interface-recovery-time 10
set protocols l2-learning vpls-mac-move virtual-mac 00:00:5e:00:01:00/40
set routing-instances vpls_1 instance-type vpls
set routing-instances vpls_1 interface xe-1/3/1.600
set routing-instances vpls_1 protocols vpls enable-mac-move-action
set routing-instances vpls_1 protocols vpls no-tunnel-services
set routing-instances vpls_1 protocols vpls vpls-id 100
set routing-instances vpls_1 protocols vpls neighbor 192.0.2.1

```

```

PE2 set interfaces xe-4/0/0 unit 0 family inet address 198.51.100.10/24
set interfaces xe-4/0/0 unit 0 family mpls
set interfaces xe-4/1/0 unit 0 family inet address 198.51.100.4/24
set interfaces xe-4/1/0 unit 0 family mpls
set interfaces xe-4/2/0 unit 0 family inet address 198.51.100.7/24
set interfaces xe-4/2/0 unit 0 family mpls
set interfaces xe-4/3/0 vlan-tagging
set interfaces xe-4/3/0 encapsulation vlan-vpls
set interfaces xe-4/3/0 unit 600 encapsulation vlan-vpls
set interfaces xe-4/3/0 unit 600 vlan-id 600
set interfaces lo0 unit 0 family inet address 192.0.2.3/24
set routing-options router-id 192.0.2.3
set routing-options autonomous-system 701
set protocols mpls interface fxp0.0 disable
set protocols mpls interface xe-4/2/0.0
set protocols mpls interface xe-4/1/0.0
set protocols mpls interface xe-4/0/0.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface xe-4/2/0.0 interface-type p2p
set protocols ospf area 0.0.0.0 interface xe-4/2/0.0 metric 10
set protocols ospf area 0.0.0.0 interface xe-4/1/0.0 interface-type p2p
set protocols ospf area 0.0.0.0 interface xe-4/1/0.0 metric 10
set protocols ospf area 0.0.0.0 interface xe-4/0/0.0 interface-type p2p
set protocols ospf area 0.0.0.0 interface xe-4/0/0.0 metric 10
set protocols ldp interface xe-4/0/0.0
set protocols ldp interface xe-4/1/0.0
set protocols ldp interface xe-4/2/0.0
set protocols ldp interface fxp0.0 disable
set protocols ldp interface lo0.0
set protocols l2-learning global-mac-move threshold-time 30
set protocols l2-learning global-mac-move threshold-count 4
set protocols l2-learning global-mac-move threshold-count 5
set protocols l2-learning vpls-mac-move cooloff-time 10
set protocols l2-learning vpls-mac-move statistical-approach-wait-time 10
set protocols l2-learning vpls-mac-move interface-recovery-time 10

```



```

set protocols l2-learning vpls-mac-move virtual-mac 00:00:5e:00:01:00/40
set routing-instances vpls_1 instance-type vpls
set routing-instances vpls_1 interface xe-4/3/0.600
set routing-instances vpls_1 protocols vpls enable-mac-move-action
set routing-instances vpls_1 protocols vpls no-tunnel-services
set routing-instances vpls_1 protocols vpls vpls-id 100
set routing-instances vpls_1 protocols vpls neighbor 192.0.2.1

```

```

PE3 set interfaces xe-1/0/0 unit 0 family inet address 198.51.100.9/24
 set interfaces xe-1/0/0 unit 0 family mpls
 set interfaces xe-1/1/0 unit 0 family inet address 198.51.100.12/24
 set interfaces xe-1/1/0 unit 0 family mpls
 set interfaces xe-1/2/0 unit 0 family inet address 198.51.100.11/24
 set interfaces xe-1/2/0 unit 0 family mpls
 set interfaces xe-1/3/0 vlan-tagging
 set interfaces xe-1/3/0 encapsulation vlan-vpls
 set interfaces xe-1/3/0 unit 600 encapsulation vlan-vpls
 set interfaces xe-1/3/0 unit 600 vlan-id 600
 set interfaces xe-2/3/0 vlan-tagging
 set interfaces xe-2/3/0 encapsulation vlan-vpls
 set interfaces xe-2/3/0 unit 600 encapsulation vlan-vpls
 set interfaces xe-2/3/0 unit 600 vlan-id 600
 set interfaces lo0 unit 0 family inet address 192.0.2.4/24
 set routing-options router-id 192.0.2.4
 set routing-options autonomous-system 701
 set protocols mpls interface fxp0.0 disable
 set protocols mpls interface xe-1/2/0.0
 set protocols mpls interface xe-1/0/0.0
 set protocols mpls interface xe-1/1/0.0
 set protocols ospf area 0.0.0.0 interface lo0.0 passive
 set protocols ospf area 0.0.0.0 interface fxp0.0 disable
 set protocols ospf area 0.0.0.0 interface xe-1/2/0.0 interface-type p2p
 set protocols ospf area 0.0.0.0 interface xe-1/2/0.0 metric 10
 set protocols ospf area 0.0.0.0 interface xe-1/0/0.0 interface-type p2p
 set protocols ospf area 0.0.0.0 interface xe-1/0/0.0 metric 10
 set protocols ospf area 0.0.0.0 interface xe-1/1/0.0 interface-type p2p
 set protocols ospf area 0.0.0.0 interface xe-1/1/0.0 metric 10
 set protocols ldp interface xe-1/0/0.0
 set protocols ldp interface xe-1/1/0.0
 set protocols ldp interface xe-1/2/0.0
 set protocols ldp interface fxp0.0 disable
 set protocols ldp interface lo0.0
 set protocols l2-learning global-mac-move threshold-time 30
 set protocols l2-learning global-mac-move threshold-count 4
 set protocols l2-learning vpls-mac-move cooloff-time 10
 set protocols l2-learning vpls-mac-move statistical-approach-wait-time 10
 set protocols l2-learning vpls-mac-move interface-recovery-time 10
 set protocols l2-learning vpls-mac-move virtual-mac 00:00:52:00:01:00/40
 set policy-options policy-statement pplb then load-balance per-packet
 set routing-instances vpls_1 instance-type vpls
 set routing-instances vpls_1 interface xe-1/3/0.600
 set routing-instances vpls_1 interface xe-2/3/0.600
 set routing-instances vpls_1 protocols vpls no-tunnel-services
 set routing-instances vpls_1 protocols vpls vpls-id 100
 set routing-instances vpls_1 protocols vpls neighbor 192.0.2.1

```

**Configuring Device PE1**

**Step-by-Step Procedure** The following example requires that you 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 Device PE1:



**NOTE:** Repeat this procedure for Routers PE0, PE2, and PE3 after modifying the appropriate interface names, addresses, and any other parameters for the router.

1. Configure the interfaces.

```
[edit interfaces]
```

```
user@PE1# set ge-0/0/3 unit 0 family inet address 198.51.100.2/24
```

```
user@PE1# set ge-0/0/3 unit 0 family mpls
```

```
user@PE1# set xe-1/2/0 unit 0 family inet address 198.51.100.5/24
```

```
user@PE1# set xe-1/2/0 unit 0 family mpls
```

```
user@PE1# set xe-1/2/1 unit 0 family inet address 198.51.100.3/24
```

```
user@PE1# set xe-1/2/1 unit 0 family mpls
```

```
user@PE1# set xe-1/3/1 vlan-tagging
```

```
user@PE1# set xe-1/3/1 encapsulation vlan-vpls
```

```
user@PE1# set xe-1/3/1 unit 600 encapsulation vlan-vpls
```

```
user@PE1# set xe-1/3/1 unit 600 vlan-id 600
```

```
user@PE1# set lo0 unit 0 family inet address 192.0.2.2/24
```

2. Configure the routing options.

```
[edit routing-options]
```

```
user@PE1# set router-id 192.0.2.2
```

```
user@PE1# set autonomous-system 701
```

3. Configure the MPLS protocol on the interface.

```
[edit protocols mpls]
```

```
user@PE1# set interface fxp0.0 disable
```

```
user@PE1# set interface ge-0/0/3.0
```

```
user@PE1# set interface xe-1/2/1.0
```

```
user@PE1# set interface xe-1/2/0.0
```

4. Configure the OSPF protocol.

```
[edit protocols ospf]
```

```
user@PE1# set area 0.0.0.0 interface lo0.0 passive
```

```
user@PE1# set area 0.0.0.0 interface fxp0.0 disable
```

```
user@PE1# set area 0.0.0.0 interface ge-0/0/3.0 interface-type p2p
```

```
user@PE1# set area 0.0.0.0 interface ge-0/0/3.0 metric 10
```

```
user@PE1# set area 0.0.0.0 interface xe-1/2/1.0 interface-type p2p
```

```

user@PE1# set area 0.0.0.0 interface xe-1/2/1.0 metric 10
user@PE1# set area 0.0.0.0 interface xe-1/2/0.0 interface-type p2p
user@PE1# set area 0.0.0.0 interface xe-1/2/0.0 metric 10

```

5. Configure the LDP protocols on the interfaces.

```

[edit protocols ldp]
user@PE1# set interface ge-0/0/3.0
user@PE1# set interface xe-1/2/0.0
user@PE1# set interface xe-1/2/1.0
user@PE1# set interface fxp0.0 disable
user@PE1# set interface lo0.0

```

6. Configure the threshold time and the threshold count to detect MAC moves.

```

[edit protocols l2-learning global-mac-move]
user@PE1# set threshold-time 30
user@PE1# set threshold-count 4

```

7. Configure VPLS MAC move parameters like cooloff time, statistical approach wait time, interface recovery time, and virtual MAC.

```

[edit protocols l2-learning vpls-mac-move]
user@PE1# set cooloff-time 10
user@PE1# set statistical-approach-wait-time 10
user@PE1# set interface-recovery-time 10
user@PE1# set virtual-mac 00:00:5e:00:01:00/40

```

8. Enable MAC move action on the interface for the VPLS instance vpls\_1.

```

[edit routing-instances vpls_1]
user@PE1# set instance-type vpls
user@PE1# set interface xe-1/3/1.600
user@PE1# set protocols vpls enable-mac-move-action
user@PE1# set protocols vpls no-tunnel-services
user@PE1# set protocols vpls vpls-id 100
user@PE1# set protocols vpls neighbor 192.0.2.1

```

### Results

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

```

user@PE1# show interfaces
ge-0/0/3 {
 unit 0 {
 family inet {
 address 198.51.100.2/24;
 }
 family mpls;
 }
}
xe-1/2/0 {
 unit 0 {
 family inet {
 address 198.51.100.5/24;
 }
 }
}

```

```
 }
 family mpls;
 }
}
xe-1/2/1 {
 unit 0 {
 family inet {
 address 198.51.100.3/24;
 }
 family mpls;
 }
}
xe-1/3/1 {
 vlan-tagging;
 encapsulation vlan-vpls;
 unit 600 {
 encapsulation vlan-vpls;
 vlan-id 600;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.2/24;
 }
 }
}

user@PE1# show protocols
mpls {
 interface fxp0.0 {
 disable;
 }
 interface ge-0/0/3.0;
 interface xe-1/2/1.0;
 interface xe-1/2/0.0;
}
ospf {
 area 0.0.0.0 {
 interface lo0.0 {
 passive;
 }
 interface fxp0.0 {
 disable;
 }
 interface ge-0/0/3.0 {
 interface-type p2p;
 metric 10;
 }
 interface xe-1/2/1.0 {
 interface-type p2p;
 metric 10;
 }
 interface xe-1/2/0.0 {
 interface-type p2p;
 metric 10;
 }
 }
}
```

```

 }
 }
}
ldp {
 interface ge-0/0/3.0;
 interface xe-1/2/0.0;
 interface xe-1/2/1.0;
 interface fxp0.0 {
 disable;
 }
 interface lo0.0;
}
l2-learning {
 global-mac-move {
 threshold-time 30;
 threshold-count 4;
 }
 vpls-mac-move {
 cooloff-time 10;
 statistical-approach-wait-time 10;
 interface-recovery-time 10;
 virtual-mac 00:00:5e:00:01:00/40;
 }
}
}

user@PE1# show routing-instances
vpls_1 {
 instance-type vpls;
 interface xe-1/3/1.600;
 protocols {
 vpls {
 enable-mac-move-action;
 no-tunnel-services;
 vpls-id 100;
 neighbor 192.0.2.1;
 }
 }
}
}

```

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

## Verification

Verify that the configuration is working properly.

- [Verifying the MAC Move in a VPLS Network on page 914](#)
- [Verifying the MAC Move in a VPLS Instance on page 914](#)
- [Verifying the MAC Move Buffer in a VPLS Network on page 914](#)
- [Verifying the VPLS MAC Table for the Base IFL Approach Algorithm on page 915](#)
- [Verifying That the Interface Is Disabled on page 916](#)
- [Verifying the VPLS MAC Table for the Statistical Approach Algorithm on page 917](#)

***Verifying the MAC Move in a VPLS Network***

**Purpose** Verify that the MAC move is observed in a VPLS network.

**Action** From operational mode, run the **show vpls mac-move-action** command for Device PE1.

```
user@PE1> show vpls mac-move-action
Instance: vpls_1
 Local interface: xe-1/3/1.600, Index: 341
 Algorithm used : Base IFL
 Time rec : 02:30:35
 Recovery timer : Yes
```

**Meaning** The output shows Instance name, Local interface and Algorithm used indicating that VPLS MAC Move is observed in a VPLS network.

***Verifying the MAC Move in a VPLS Instance***

**Purpose** Verify that the MAC move is observed in a VPLS instance.

**Action** From operational mode, run the **show vpls mac-move-action instance *instance-name*** command for Device PE1.

```
user@PE1> show vpls mac-move-action instance vpls_1

Instance: vpls_1
 Local interface: xe-1/3/1.600, Index: 341
 Algorithm used : Base IFL
 Time rec : 02:29:35
 Recovery timer : Yes
```

**Meaning** The output shows Local interface, and Algorithm used indicating that VPLS MAC move has been observed in a VPLS instance.

***Verifying the MAC Move Buffer in a VPLS Network***

**Purpose** Verify the MAC move buffer to monitor the MAC moves that are occurring in the VPLS network.

**Action** From operational mode, run the **show l2-learning mac-move-buffer** command for Device PE1.

```
user@PE1> show l2-learning mac-move-buffer
```

| MAC<br>Address    | Time<br>Rec. | Bridge<br>Domain |
|-------------------|--------------|------------------|
| 00:10:00:01:00:09 | 03:26:00     | __vpls_1__       |
| 00:10:00:01:00:05 | 03:26:00     | __vpls_1__       |
| 00:10:00:01:00:03 | 03:26:00     | __vpls_1__       |
| 00:10:00:01:00:05 | 03:26:00     | __vpls_1__       |
| 00:10:00:01:00:08 | 03:26:00     | __vpls_1__       |
| 00:10:00:01:00:01 | 03:26:00     | __vpls_1__       |
| 00:10:00:01:00:03 | 03:26:00     | __vpls_1__       |
| 00:10:00:01:00:01 | 03:26:00     | __vpls_1__       |
| 00:10:00:01:00:00 | 03:26:00     | __vpls_1__       |
| 00:10:00:01:00:01 | 03:26:01     | __vpls_1__       |
| 00:10:00:01:00:06 | 03:26:01     | __vpls_1__       |
| 00:10:00:01:00:02 | 03:26:01     | __vpls_1__       |
| 00:10:00:01:00:08 | 03:26:01     | __vpls_1__       |
| 00:10:00:01:00:00 | 03:26:01     | __vpls_1__       |
| 00:10:00:01:00:01 | 03:26:01     | __vpls_1__       |
| 00:10:00:01:00:09 | 03:26:01     | __vpls_1__       |

#### *Verifying the VPLS MAC Table for the Base IFL Approach Algorithm*

**Purpose** Verify the base learning interfaces for the MAC addresses. .

**Action** From operational mode, run the **show vpls mac-table extensive** command to obtain extensive information of VPLS MAC table.

```
user@PE1> show vpls mac-table extensive
```

```
MAC address: 00:10:00:01:00:00
 Routing instance: vpls_1
 Bridging domain: __vpls_1__, VLAN : NA
 Learning interface: lsi.1049165
 Base learning interface: lsi.1049165
 Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
 Epoch: 0 Sequence number: 1
 Learning mask: 0x00000001

MAC address: 00:10:00:01:00:01
 Routing instance: vpls_1
 Bridging domain: __vpls_1__, VLAN : NA
 Learning interface: lsi.1049165
 Base learning interface: lsi.1049165
 Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
 Epoch: 0 Sequence number: 1
 Learning mask: 0x00000001

MAC address: 00:10:00:01:00:02
 Routing instance: vpls_1
 Bridging domain: __vpls_1__, VLAN : NA
 Learning interface: lsi.1049165
 Base learning interface: lsi.1049165
 Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
 Epoch: 0 Sequence number: 1
 Learning mask: 0x00000001

MAC address: 00:10:00:01:00:03
 Routing instance: vpls_1
 Bridging domain: __vpls_1__, VLAN : NA
 Learning interface: lsi.1049165
 Base learning interface: lsi.1049165
 Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
 Epoch: 0 Sequence number: 1
 Learning mask: 0x00000001
```

**Meaning** The output of the command **show vpls mac-table extensive** shows the base learning interface of the MAC address.

#### ***Verifying That the Interface Is Disabled***

**Purpose** Verify that the base learning interface of the MAC address is disabled.



**Action** From operational mode, run the **show interfaces *interface-name*** command for Device PE1.

```
user@PE1> show interfaces xe-1/3/1.600
```

```
Logical interface xe-1/3/1.600 (Index 341) (SNMP ifIndex 2864)
 Flags: Up Link-Layer-Down SNMP-Traps 0x4000 VLAN-Tag [0x8100.600]
Encapsulation: VLAN-VPLS
Input packets : 2234018970
Output packets: 2234728895
Protocol vpls, MTU: 1518
Flags: Is-Primary
```

**Meaning** The flag **link-layer-down** in the output indicates that the interface is disabled.

### *Verifying the VPLS MAC Table for the Statistical Approach Algorithm*

**Purpose** Verify the VPLS MAC table for the statistical approach algorithm.

**Action** From operational mode, run the **show vpls mac-table extensive** command for Device PE1.

```
user@PE1> show vpls mac-table extensive
```

```
MAC address: 00:10:00:01:00:00
 Routing instance: vpls_1
 Bridging domain: __vpls_1__, VLAN : NA
 Learning interface: xe-1/3/1.600
 Base learning interface: NULL
 Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
 Epoch: 3 Sequence number: 442
 Learning mask: 0x00000002
```

```
MAC address: 00:10:00:01:00:01
 Routing instance: vpls_1
 Bridging domain: __vpls_1__, VLAN : NA
 Learning interface: xe-1/3/1.600
 Base learning interface: NULL
 Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
 Epoch: 3 Sequence number: 442
 Learning mask: 0x00000003
```

```
MAC address: 00:10:00:01:00:02
 Routing instance: vpls_1
 Bridging domain: __vpls_1__, VLAN : NA
 Learning interface: xe-1/3/1.600
 Base learning interface: NULL
 Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
 Epoch: 3 Sequence number: 442
 Learning mask: 0x00000002
```

```
MAC address: 00:10:00:01:00:03
 Routing instance: vpls_1
 Bridging domain: __vpls_1__, VLAN : NA
 Learning interface: xe-1/3/1.600
 Base learning interface: NULL
 Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
 Epoch: 3 Sequence number: 442
 Learning mask: 0x00000002
```

**Meaning** The **Base learning interface** is null which indicates that the statistical approach is in use.

## Configuring Improved VPLS MAC Address Learning on T4000 Routers with Type 5 FPCs

Junos OS Release 12.3 enables improved virtual private LAN service (VPLS) MAC address learning on T4000 routers with Type 5 FPCs by supporting up to 262,143 MAC addresses per VPLS routing instance. In Junos OS releases before Release 12.3, T4000 routers with Type 5 FPCs support only 65,535 MAC addresses per VPLS routing instance.

Before you begin, configure VPLS. See “[Configuring VPLS Routing Instances](#)” on page 563.

To enable improved VPLS MAC address learning on T4000 routers with Type 5 FPCs:

1. Enable the network services mode by including the **enhanced-mode** statement at the **[edit chassis network-services]** hierarchy level.

```
[edit chassis network-services]
user@host# set enhanced-mode
```



**NOTE:** After you configure the **enhanced-mode** statement and commit your configuration, a warning message prompts you to reboot the router.

2. Perform a system reboot in operational mode.

```
user@host> request system-reboot
```

After the router reboots, only the T4000 Type 5 FPCs are online while the remaining FPCs are offline. You can verify the status of the FPCs by using the **show chassis fpc** operational mode command.

3. Modify the size of the VPLS MAC address table at the **[edit routing-instance instance-name protocols vpls]** hierarchy level.

```
[edit routing-instance instance-name protocols vpls]
user@host# set mac-table-size size
```

For example, to set the MAC address learning limit to 262,143 addresses for each **vpls** routing instance:

```
[edit routing-instance vpls protocols vpls]
user@host# set mac-table-size 262143
```



**NOTE:** The **enhanced-mode** statement supports up to 262,143 MAC addresses per VPLS routing instance. However, the MAC address learning limit for each interface remains the same (that is, 65,535 MAC addresses).

4. In configuration mode, verify the configuration.

```
user@host# show routing-instances instance-name
vpls {
 instance-type vpls;
```

```
protocols {
 vpls {
 mac-table-size {
 262143;
 }
 }
}
```

To disable the improved VPLS MAC address learning feature on T4000 routers with Type 5 FPCs, include the **delete chassis network-services enhanced-mode** statement at the **[edit]** hierarchy level.



**NOTE:** After you disable network services mode and commit your configuration, a warning message prompts you to reboot the router. You must reboot the router. Continuing without a reboot might result in unexpected system behavior.

#### Related Documentation

- *enhanced-mode*
- *Network Services Mode Overview*
- [Configuring VPLS Routing Instances on page 563](#)
- *show chassis fpc*



# Configuring Class of Service and Firewall Filters in VPLS

- [Configuring EXP-Based Traffic Classification for VPLS on page 921](#)
- [Configuring Firewall Filters and Policers for VPLS on page 921](#)
- [Firewall Filter Match Conditions for VPLS Traffic on page 926](#)

## Configuring EXP-Based Traffic Classification for VPLS

---

You can enable EXP classification on traffic entering core facing VPLS LSI interfaces on a VPLS routing instance by configuring either a logical tunnel interface (**lt-**) or the **no-tunnel-services** statement. By configuring either of these, a default EXP classifier is enabled on every core facing interface that includes **family mpls** in its configuration. This feature works on MX Series routers and EX Series switches only. You can configure an EXP classifier explicitly at the **[edit class-of-service]** hierarchy level. For more information about EXP classifiers, see the *Class of Service Feature Guide for Routing Devices*.

To enable EXP classification on traffic entering core facing VPLS LSI interfaces on a VPLS routing instance, include the **no-tunnel-services** statement:

```
no-tunnel-services;
```

You can include this statement at the following hierarchy levels:

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

## Configuring Firewall Filters and Policers for VPLS

---

You can configure both firewall filters and policers for VPLS. Firewall filters allow you to filter packets based on their components and to perform an action on packets that match the filter. Policers allow you to limit the amount of traffic that passes into or out of an interface.

VPLS filters and policers act on a Layer 2 frame that includes the media access control (MAC) header (after any VLAN rewrite or other rules are applied), but does not include the cyclical redundancy check (CRC) field.

You can apply VPLS filters and policers on the PE router to customer-facing interfaces only.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.



**NOTE:** The behavior of firewall filters processing with MAC addresses differs between DPCs and MPCs. On MPCs, interface filters are always applied before MAC learning occurs. The input forwarding table filter is applied after MAC learning is completed. However, on DPCs, MAC learning occurs independently of the application of filters. If the CE-facing interface of the PE where the firewall filter is applied is an MPC, then the MAC entry times out and is never learned again. However, if the CE-facing interface of the PE where the firewall filter is applied is an DP, then the MAC entry is not timed out and if the MAC address entry is manually cleared, it is relearned.

The following sections explain how to configure filters and policers for VPLS:

- [Configuring a VPLS Filter on page 922](#)
- [Configuring a VPLS Policer on page 925](#)

## Configuring a VPLS Filter

To configure a filter for VPLS, include the **filter** statement at the **[edit firewall family vpls]** hierarchy level:

```
[edit firewall family vpls]
filter filter-name {
 interface-specific;
 term term-name {
 from {
 match-conditions;
 }
 then {
 actions;
 }
 }
}
```

For more information about how to configure firewall filters, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*. For information on how to configure a VPLS filter match condition, see [“Firewall Filter Match Conditions for VPLS Traffic” on page 926](#).

To configure a filter for VPLS traffic, complete the following tasks:

- [Configuring an Interface-Specific Counter for VPLS on page 923](#)
- [Configuring an Action for the VPLS Filter on page 923](#)
- [Configuring VPLS FTFs on page 923](#)

- [Changing Precedence for Spanning-Tree BPDU Packets on page 923](#)
- [Applying a VPLS Filter to an Interface on page 924](#)
- [Applying a VPLS Filter to a VPLS Routing Instance on page 924](#)
- [Configuring a Filter for Flooded Traffic on page 924](#)

---

### Configuring an Interface-Specific Counter for VPLS

When you configure a firewall filter for VPLS and apply it to multiple interfaces, you can specify individual counters specific to each interface. This allows you to collect separate statistics on the traffic transiting each interface.

To generate an interface-specific counter for VPLS, you configure the **interface-specific** statement. A separate instantiation of the filter is generated. This filter instance has a different name (based on the interface name) and collects statistics on the interface specified only.

To configure interface-specific counters, include the **interface-specific** statement at the **[edit firewall family vpls filter *filter-name*]** hierarchy level:

```
[edit firewall family vpls filter filter-name]
interface-specific;
```



**NOTE:** The counter name is restricted to 24 bytes. If the renamed counter exceeds this maximum length, it might be rejected.

---

### Configuring an Action for the VPLS Filter

You can configure the following actions for a VPLS filter at the **[edit firewall family vpls filter *filter-name* term *term-name* then]** hierarchy level: **accept**, **count**, **discard**, **forwarding-class**, **loss-priority**, **next**, **policer**.

---

### Configuring VPLS FTFs

Forwarding table filters (FTFs) are filters configured for forwarding tables. For VPLS, they are attached to the destination MAC (DMAC) forwarding table of the VPLS routing instance. You define VPLS FTFs in the same manner as any other type of FTF. You can only apply a VPLS FTF as an input filter.

To specify a VPLS FTF, include the **filter input** statement at the **[edit routing-instance *routing-instance-name* forwarding-options family vpls]** hierarchy level:

```
[edit routing-instance routing-instance-name forwarding-options family vpls]
filter input filter-name;
```

---

### Changing Precedence for Spanning-Tree BPDU Packets

Spanning tree BPDU packets are automatically set to a high precedence. The queue number on these packets is set to 3. On M Series routers (except the M320 router) by default, a queue value of 3 indicates high precedence. To enable this higher precedence on BPDU packets, an instance-specific BPDU precedence filter named **default\_bpdu\_filter**

is automatically attached to the VPLS DMAC table. This filter places a high precedence on all packets sent to **01:80:c2:00:00:00/24**.

You can overwrite this filter by configuring a VPLS FTF filter and applying it to the VPLS routing instance. For more information, see [“Configuring VPLS FTFs” on page 923](#) and [“Applying a VPLS Filter to a VPLS Routing Instance” on page 924](#).

---

### Applying a VPLS Filter to an Interface

To apply a VPLS filter to an interface, include the **filter** statement:

```
filter {
 group index;
 input input-filter-name;
 output output-filter-name;
}
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *number* family vpls]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *number* family vpls]

In the **input** statement, list the name of the VPLS filter to be evaluated when packets are received on the interface. In the **output** statement, list the name of the VPLS filter to be evaluated when packets are transmitted on the interface.



**NOTE:** For output interface filters, MAC addresses are learned after the filter action is completed. When an output interface filter's action is **discard**, the packet is dropped before the MAC address is learned. However, an input interface filter learns the MAC address before discarding the packet.

---

### Applying a VPLS Filter to a VPLS Routing Instance

You can apply a VPLS filter to a VPLS routing instance. The filter checks traffic passing through the specified routing instance.

Input routing instance filters learn the MAC address before the filter action is completed, so if the filter action is **discard**, the MAC address is learned before the packet is dropped.

To apply a VPLS filter to packets arriving at a VPLS routing instance and specify the filter, include the **filter input** statement at the [edit routing-instances *routing-instance-name* forwarding-options family vpls] hierarchy level:

```
[edit routing-instances routing-instance-name forwarding-options family vpls]
filter input input-filter-name;
```

---

### Configuring a Filter for Flooded Traffic

You can configure a VPLS filter to filter flooded packets. CE routers typically flood the following types of packets to PE routers in VPLS routing instances:



- Layer 2 broadcast packets
- Layer 2 multicast packets
- Layer 2 unicast packets with an unknown destination MAC address
- Layer 2 packets with a MAC entry in the DMAC routing table

You can configure filters to manage how these flooded packets are distributed to the other PE routers in the VPLS routing instance.

To apply a flooding filter to packets arriving at the PE router in the VPLS routing instance, and specify the filter, include the **flood input** statement:

```
flood input filter-name;
```

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* forwarding-options family vpls]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options family vpls]

## Configuring a VPLS Policer

You can configure a policer for VPLS traffic. The VPLS policer configuration is similar to the configuration of any other type of policer.

VPLS policers have the following characteristics:

- You cannot police the default VPLS routes stored in the flood table from PE router-sourced flood traffic.
- When specifying policing bandwidth, the VPLS policer considers all Layer 2 bytes in a packet to determine the packet length.

To configure a VPLS policer, include the **policer** statement at the [edit firewall] hierarchy level:

```
[edit firewall]
policer policer-name {
 bandwidth-limit limit;
 burst-size-limit limit;
 then action;
}
```

To apply a VPLS policer to an interface, include the **policer** statement:

```
policer {
 input input-policer-name;
 output output-policer-name;
}
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *number* family vpls]

- `[edit logical-systems logical-system-name interfaces interface-name unit number family vpls`

In the **input** statement, list the name of the VPLS policer to be evaluated when packets are received on the interface. In the **output** statement, list the name of the VPLS policer to be evaluated when packets are transmitted on the interface. This type of VPLS policer can only apply to unicast packets. For information about how to filter flood packets, see [“Configuring a Filter for Flooded Traffic” on page 924](#).

**Related  
Documentation**

- [Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices](#)
- [Firewall Filter Match Conditions for VPLS Traffic on page 926](#)

---

## Firewall Filter Match Conditions for VPLS Traffic

In the **from** statement in the VPLS filter term, you specify conditions that the packet must match for the action in the **then** statement to be taken. All conditions in the **from** statement must match for the action to be taken. The order in which you specify match conditions is not important, because a packet must match all the conditions in a term for a match to occur.

If you specify no match conditions in a term, that term matches all packets.

An individual condition in a **from** statement can contain a list of values. For example, you can specify numeric ranges. You can also specify multiple source addresses or destination addresses. When a condition defines a list of values, a match occurs if one of the values in the list matches the packet.

Individual conditions in a **from** statement can be negated. When you negate a condition, you are defining an explicit mismatch. For example, the negated match condition for **forwarding-class** is **forwarding-class-except**. If a packet matches a negated condition, it is immediately considered not to match the **from** statement, and the next term in the filter is evaluated, if there is one. If there are no more terms, the packet is discarded.

You can configure a firewall filter with match conditions for Virtual Private LAN Service (VPLS) traffic (**family vpls**). [Table 23 on page 927](#) describes the **match-conditions** you can configure at the `[edit firewall family vpls filter filter-name term term-name from]` hierarchy level.



**NOTE:** Not all match conditions for VPLS traffic are supported on all routing platforms or switching platforms. A number of match conditions for VPLS traffic are supported only on MX Series 3D Universal Edge Routers.

In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

---

Table 23: Firewall Filter Match Conditions for VPLS Traffic

| Match Condition                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>destination-mac-address address</b>     | Match the destination media access control (MAC) address of a VPLS packet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>destination-port number</b>             | <p>(MX Series routers and EX Series switches only) Match the UDP or TCP destination port field.</p> <p>You cannot specify both the <b>port</b> and <b>destination-port</b> match conditions in the same term.</p> <p>In place of the numeric value, you can specify one of the following text synonyms (the port numbers are also listed): <b>afs</b> (1483), <b>bgp</b> (179), <b>biff</b> (512), <b>bootpc</b> (68), <b>bootps</b> (67), <b>cmd</b> (514), <b>cvspserver</b> (2401), <b>dhcp</b> (67), <b>domain</b> (53), <b>eklogin</b> (2105), <b>ekshell</b> (2106), <b>exec</b> (512), <b>finger</b> (79), <b>ftp</b> (21), <b>ftp-data</b> (20), <b>http</b> (80), <b>https</b> (443), <b>ident</b> (113), <b>imap</b> (143), <b>kerberos-sec</b> (88), <b>klogin</b> (543), <b>kpasswd</b> (761), <b>krb-prop</b> (754), <b>krbupdate</b> (760), <b>kshell</b> (544), <b>ldap</b> (389), <b>ldp</b> (646), <b>login</b> (513), <b>mobileip-agent</b> (434), <b>mobilip-mn</b> (435), <b>msdp</b> (639), <b>netbios-dgm</b> (138), <b>netbios-ns</b> (137), <b>netbios-ssn</b> (139), <b>nfsd</b> (2049), <b>nntp</b> (119), <b>ntalk</b> (518), <b>ntp</b> (123), <b>pop3</b> (110), <b>pptp</b> (1723), <b>printer</b> (515), <b>radacct</b> (1813), <b>radius</b> (1812), <b>rip</b> (520), <b>rkinit</b> (2108), <b>smtp</b> (25), <b>snmp</b> (161), <b>snmptrap</b> (162), <b>snpp</b> (444), <b>socks</b> (1080), <b>ssh</b> (22), <b>sunrpc</b> (111), <b>syslog</b> (514), <b>tacacs</b> (49), <b>tacacs-ds</b> (65), <b>talk</b> (517), <b>telnet</b> (23), <b>tftp</b> (69), <b>timed</b> (525), <b>who</b> (513), or <b>xmcp</b> (177).</p> |
| <b>destination-port-except number</b>      | (MX Series routers and EX Series switches only) Do not match on the TCP or UDP destination port field. You cannot specify both the <b>port</b> and <b>destination-port</b> match conditions in the same term.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>destination-prefix-list name</b>        | <p>(MX Series routers and EX Series switches only) Match destination prefixes in the specified list. Specify the name of a prefix list defined at the <b>[edit policy-options prefix-list prefix-list-name]</b> hierarchy level.</p> <p><b>NOTE:</b> VPLS prefix lists support only IPv4 addresses. IPv6 addresses included in a VPLS prefix list will be discarded.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>destination-prefix-list name except</b> | (MX Series routers and EX Series switches only) Do not match destination prefixes in the specified list. For more information, see the <b>destination-prefix-list</b> match condition.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>dscp number</b>                         | <p>(MX Series routers and EX Series switches only) Match the Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most significant 6 bits of this byte form the DSCP. For more information, see the <i>Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic</i>.</p> <p>You can specify a numeric value from <b>0</b> through <b>63</b>. To specify the value in hexadecimal form, include <b>0x</b> as a prefix. To specify the value in binary form, include <b>b</b> as a prefix.</p> <p>In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed):</p> <ul style="list-style-type: none"> <li>RFC 3246, <i>An Expedited Forwarding PHB (Per-Hop Behavior)</i>, defines one code point: <b>ef</b> (46).</li> <li>RFC 2597, <i>Assured Forwarding PHB Group</i>, defines 4 classes, with 3 drop precedences in each class, for a total of 12 code points:</li> </ul> <p><b>af11</b> (10), <b>af12</b> (12), <b>af13</b> (14),</p> <p><b>af21</b> (18), <b>af22</b> (20), <b>af23</b> (22),</p> <p><b>af31</b> (26), <b>af32</b> (28), <b>af33</b> (30),</p> <p><b>af41</b> (34), <b>af42</b> (36), <b>af43</b> (38)</p>                                                                                                                                                                                                                                                                                                                                                                               |

Table 23: Firewall Filter Match Conditions for VPLS Traffic (*continued*)

| Match Condition                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| <b>dscp-except <i>number</i></b>        | (MX Series routers and EX Series switches only) Do not match on the DSCP. For details, see the <b>dscp</b> match condition.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                |
| <b>ether-type <i>values</i></b>         | <p>Match the 2-octet IEEE 802.3 Length/EtherType field to the specified value or list of values.</p> <p>You can specify decimal or hexadecimal values from 0 through 65535 (0xFFFF). A value from 0 through 1500 (0x05DC) specifies the length of an Ethernet Version 1 frame. A value from 1536 (0x0600) through 65535 specifies the EtherType (nature of the MAC client protocol) of an Ethernet Version 2 frame.</p> <p>In place of the numeric value, you can specify one of the following text synonyms (the hexadecimal values are also listed): <b>aarp</b> (0x80F3), <b>appletalk</b> (0x809B), <b>arp</b> (0x0806), <b>ipv4</b> (0x0800), <b>ipv6</b> (0x86DD), <b>mpls-multicast</b> (0x8848), <b>mpls-unicast</b> (0x8847), <b>oam</b> (0x8902), <b>ppp</b> (0x880B), <b>pppoe-discovery</b> (0x8863), <b>pppoe-session</b> (0x8864), or <b>sna</b> (0x80D5).</p> |                                                                                |
| <b>ether-type-except <i>values</i></b>  | <p>Do not match the 2-octet Length/EtherType field to the specified value or list of values.</p> <p>For details about specifying the <b>values</b>, see the <b>ether-type</b> match condition.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                |
| <b>flexible-match-mask <i>value</i></b> | <b>bit-length</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Length of the data to be matched in bits, not needed for string input (0..128) |
|                                         | <b>bit-offset</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Bit offset after the (match-start + byte) offset (0..7)                        |
|                                         | <b>byte-offset</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Byte offset after the match start point                                        |
|                                         | <b>flexible-mask-name</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Select a flexible match from predefined template field                         |
|                                         | <b>mask-in-hex</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Mask out bits in the packet data to be matched                                 |
|                                         | <b>match-start</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Start point to match in packet                                                 |
|                                         | <b>prefix</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Value data/string to be matched                                                |

Table 23: Firewall Filter Match Conditions for VPLS Traffic (*continued*)

| Match Condition                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>flexible-match-range</b> <i>value</i>    | <b>bit-length</b><br>Length of the data to be matched in bits (0..32)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                                             | <b>bit-offset</b><br>Bit offset after the (match-start + byte) offset (0..7)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                                             | <b>byte-offset</b><br>Byte offset after the match start point                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                                             | <b>flexible-range-name</b><br>Select a flexible match from predefined template field                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                             | <b>match-start</b><br>Start point to match in packet                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                             | <b>range</b><br>Range of values to be matched                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                                             | <b>range-except</b><br>Do not match this range of values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>forwarding-class</b> <i>class</i>        | Match the forwarding class. Specify <b>assured-forwarding</b> , <b>best-effort</b> , <b>expedited-forwarding</b> , or <b>network-control</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>forwarding-class-except</b> <i>class</i> | Do not match the forwarding class. For details, see the <b>forwarding-class</b> match condition.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>icmp-code</b> <i>message-code</i>        | <p>Match the ICMP message code field.</p> <p>If you configure this match condition, we recommend that you also configure the <b>next-header icmp</b> or <b>next-header icmp6</b> match condition in the same term.</p> <p>If you configure this match condition, you must also configure the <b>icmp-type message-type</b> match condition in the same term. An ICMP message code provides more specific information than an ICMP message type, but the meaning of an ICMP message code is dependent on the associated ICMP message type.</p> <p>In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed). The keywords are grouped by the ICMP type with which they are associated:</p> <ul style="list-style-type: none"> <li>parameter-problem: <b>ip6-header-bad</b> (0), <b>unrecognized-next-header</b> (1), <b>unrecognized-option</b> (2)</li> <li>time-exceeded: <b>ttl-eq-zero-during-reassembly</b> (1), <b>ttl-eq-zero-during-transit</b> (0)</li> <li>destination-unreachable: <b>address-unreachable</b> (3), <b>administratively-prohibited</b> (1), <b>no-route-to-destination</b> (0), <b>port-unreachable</b> (4)</li> </ul> |
| <b>icmp-code-except</b> <i>message-code</i> | Do not match the ICMP message code field. For details, see the <b>icmp-code</b> match condition.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

Table 23: Firewall Filter Match Conditions for VPLS Traffic (*continued*)

| Match Condition                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>icmp-code <i>number</i></b>             | <p>(MX Series routers and EX Series switches only) Match the ICMP message code field.</p> <p>If you configure this match condition, we recommend that you also configure the <b>ip-protocol icmp</b> or <b>ip-protocol icmp6</b> match condition in the same term.</p> <p>If you configure this match condition, you must also configure the <b>icmp-type <i>message-type</i></b> match condition in the same term. An ICMP message code provides more specific information than an ICMP message type, but the meaning of an ICMP message code is dependent on the associated ICMP message type.</p> <p>In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed). The keywords are grouped by the ICMP type with which they are associated:</p> <ul style="list-style-type: none"> <li>parameter-problem: <b>ip6-header-bad</b> (0), <b>unrecognized-next-header</b> (1), <b>unrecognized-option</b> (2)</li> <li>time-exceeded: <b>ttl-eq-zero-during-reassembly</b> (1), <b>ttl-eq-zero-during-transit</b> (0)</li> <li>destination-unreachable: <b>address-unreachable</b> (3), <b>administratively-prohibited</b> (1), <b>no-route-to-destination</b> (0), <b>port-unreachable</b> (4)</li> </ul> |
| <b>icmp-code-except <i>number</i></b>      | <p>(MX Series routers and EX Series switches only) Do not match on the ICMP code field. For details, see the <b>icmp-code</b> match condition.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>icmp-type <i>number</i></b>             | <p>(MX Series routers and EX Series switches only) Match the ICMP message type field.</p> <p>If you configure this match condition, we recommend that you also configure the <b>ip-protocol icmp</b>, <b>ip-protocol icmp6</b>, or <b>ip-protocol icmpv6</b> match condition in the same term.</p> <p>In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): <b>destination-unreachable</b> (1), <b>echo-reply</b> (129), <b>echo-request</b> (128), <b>membership-query</b> (130), <b>membership-report</b> (131), <b>membership-termination</b> (132), <b>neighbor-advertisement</b> (136), <b>neighbor-solicit</b> (135), <b>node-information-reply</b> (140), <b>node-information-request</b> (139), <b>packet-too-big</b> (2), <b>parameter-problem</b> (4), <b>redirect</b> (137), <b>router-advertisement</b> (134), <b>router-renumbering</b> (138), <b>router-solicit</b> (133), or <b>time-exceeded</b> (3).</p>                                                                                                                                                                                                                                                                         |
| <b>icmp-type-except <i>number</i></b>      | <p>(MX Series routers and EX Series switches only) Do not match the ICMP message type field. For details, see the <b>icmp-type</b> match condition.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>interface <i>interface-name</i></b>     | <p>Interface on which the packet was received. You can configure a match condition that matches packets based on the interface on which they were received.</p> <p><b>NOTE:</b> If you configure this match condition with an interface that does not exist, the term does not match any packet.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>interface-group <i>group-number</i></b> | <p>Match the logical interface on which the packet was received to the specified interface group or set of interface groups. For <b>group-number</b>, specify a single value or a range of values from 0 through 255.</p> <p>To assign a logical interface to an interface group <b>group-number</b>, specify the <b>group-number</b> at the [interfaces <b>interface-name</b> unit <b>number</b> family <b>family</b> filter group] hierarchy level.</p> <p>For more information, see <i>Filtering Packets Received on a Set of Interface Groups Overview</i>.</p> <p><b>NOTE:</b> This match condition is not supported on T4000 Type 5 FPCs.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

Table 23: Firewall Filter Match Conditions for VPLS Traffic (*continued*)

| Match Condition                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>interface-group-except</b><br><i>group-name</i>        | Do not match the logical interface on which the packet was received to the specified interface group or set of interface groups. For details, see the <b>interface-group</b> match condition.<br><br><b>NOTE:</b> This match condition is not supported on T4000 Type 5 FPCs.                                                                                                                                         |
| <b>interface-set</b><br><i>interface-set-name</i>         | Match the interface on which the packet was received to the specified interface set.<br><br>To define an interface set, include the <b>interface-set</b> statement at the <b>[edit firewall]</b> hierarchy level. For more information, see <i>Filtering Packets Received on an Interface Set Overview</i> .                                                                                                          |
| <b>ip-address</b> <i>address</i>                          | (MX Series routers and EX Series switches only) 32-bit address that supports the standard syntax for IPv4 addresses.                                                                                                                                                                                                                                                                                                  |
| <b>ip-destination-address</b><br><i>address</i>           | (MX Series routers and EX Series switches only) 32-bit address that is the final destination node address for the packet.                                                                                                                                                                                                                                                                                             |
| <b>ip-precedence</b><br><i>ip-precedence-field</i>        | (MX Series routers and EX Series switches only) IP precedence field. In place of the numeric field value, you can specify one of the following text synonyms (the field values are also listed): <b>critical-ecp</b> (0xa0), <b>flash</b> (0x60), <b>flash-override</b> (0x80), <b>immediate</b> (0x40), <b>internet-control</b> (0xc0), <b>net-control</b> (0xe0), <b>priority</b> (0x20), or <b>routine</b> (0x00). |
| <b>ip-precedence-except</b><br><i>ip-precedence-field</i> | (MX Series routers and EX Series switches only) Do not match on the IP precedence field.                                                                                                                                                                                                                                                                                                                              |
| <b>ip-protocol</b> <i>number</i>                          | (MX Series routers and EX Series switches only) IP protocol field.                                                                                                                                                                                                                                                                                                                                                    |
| <b>ipv6-address</b> <i>address</i>                        | (MX Series only) 128-bit address that supports the standard syntax for IPv6 addresses.                                                                                                                                                                                                                                                                                                                                |
| <b>ip-protocol-except</b> <i>number</i>                   | (MX Series routers and EX Series switches only) Do not match on the IP protocol field.                                                                                                                                                                                                                                                                                                                                |
| <b>ipv6-destination-address</b><br><i>address</i>         | (MX Series only) 128-bit address that is the final destination node address for this packet.                                                                                                                                                                                                                                                                                                                          |
| <b>ipv6-destination-prefix-list</b><br><i>named-list</i>  | (MX Series only) Match the IPv6 destination addresses in a <i>named-list</i> .                                                                                                                                                                                                                                                                                                                                        |

Table 23: Firewall Filter Match Conditions for VPLS Traffic (*continued*)

| Match Condition                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6-next-header <i>protocol</i></b>        | <p>(MX Series only) Match IPv6 next header protocol type.</p> <p>The following list shows the supported values for <i>protocol</i>:</p> <ul style="list-style-type: none"> <li>• <b>ah</b>—IP Security authentication header</li> <li>• <b>dstopts</b>—IPv6 destination options</li> <li>• <b>egp</b>—Exterior gateway protocol</li> <li>• <b>esp</b>—IPSec Encapsulating Security Payload</li> <li>• <b>fragment</b>—IPv6 fragment header</li> <li>• <b>gre</b>—Generic routing encapsulation</li> <li>• <b>hop-by-hop</b>—IPv6 hop by hop options</li> <li>• <b>icmp</b>—Internet Control Message Protocol</li> <li>• <b>icmp6</b>—Internet Control Message Protocol Version 6</li> <li>• <b>igmp</b>—Internet Group Management Protocol</li> <li>• <b>ipip</b>—IP in IP</li> <li>• <b>ipv6</b>—IPv6 in IP</li> <li>• <b>no-next-header</b>—IPv6 no next header</li> <li>• <b>ospf</b>—Open Shortest Path First</li> <li>• <b>pim</b>—Protocol Independent Multicast</li> <li>• <b>routing</b>—IPv6 routing header</li> <li>• <b>rsvp</b>—Resource Reservation Protocol</li> <li>• <b>sctp</b>—Stream Control Transmission Protocol</li> <li>• <b>tcp</b>—Transmission Control Protocol</li> <li>• <b>udp</b>—User Datagram Protocol</li> <li>• <b>vrp</b>—Virtual Router Redundancy Protocol</li> </ul> |
| <b>ipv6-next-header-except <i>protocol</i></b> | <p>(MX Series only) Do not match the IPv6 next header protocol type.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |



Table 23: Firewall Filter Match Conditions for VPLS Traffic (*continued*)

| Match Condition                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6-payload-protocol</b><br><i>protocol</i>        | <p>(MX Series only) Match IPv6 payload protocol type.</p> <p>The following list shows the supported values for <i>protocol</i>:</p> <ul style="list-style-type: none"> <li>• <b>ah</b>—IP Security authentication header</li> <li>• <b>dstop</b>—IPv6 destination options</li> <li>• <b>egp</b>—Exterior gateway protocol</li> <li>• <b>esp</b>—IPSec Encapsulating Security Payload</li> <li>• <b>fragment</b>—IPv6 fragment header</li> <li>• <b>gre</b>—Generic routing encapsulation</li> <li>• <b>hop-by-hop</b>—IPv6 hop by hop options</li> <li>• <b>icmp</b>—Internet Control Message Protocol</li> <li>• <b>icmp6</b>—Internet Control Message Protocol Version 6</li> <li>• <b>igmp</b>—Internet Group Management Protocol</li> <li>• <b>ipip</b>—IP in IP</li> <li>• <b>ipv6</b>—IPv6 in IP</li> <li>• <b>no-next-header</b>—IPv6 no next header</li> <li>• <b>ospf</b>—Open Shortest Path First</li> <li>• <b>pim</b>—Protocol Independent Multicast</li> <li>• <b>routing</b>—IPv6 routing header</li> <li>• <b>rsvp</b>—Resource Reservation Protocol</li> <li>• <b>sctp</b>—Stream Control Transmission Protocol</li> <li>• <b>tcp</b>—Transmission Control Protocol</li> <li>• <b>udp</b>—User Datagram Protocol</li> <li>• <b>vrp</b>—Virtual Router Redundancy Protocol</li> </ul> |
| <b>ipv6-payload-protocol-except</b><br><i>protocol</i> | (MX Series only) Do not match the IPv6 payload protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>ipv6-prefix-list</b> <i>named-list</i>              | (MX Series only) Match the IPv6 address in a <i>named-list</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>ipv6-source-address</b> <i>address</i>              | (MX Series only) 128-bit address that is the originating source node address for this packet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>ipv6-source-prefix-list</b><br><i>named-list</i>    | (MX Series only) Match the IPv6 source address in a <i>named-list</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Table 23: Firewall Filter Match Conditions for VPLS Traffic (*continued*)

| Match Condition                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6-traffic-class</b> <i>number</i>            | <p>(MX Series only) Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most significant 6 bits of this byte form the DSCP. For more information, see <i>Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic</i>.</p> <p>You can specify a numeric value from <b>0</b> through <b>63</b>. To specify the value in hexadecimal form, include <b>0x</b> as a prefix. To specify the value in binary form, include <b>b</b> as a prefix.</p> <p>In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed):</p> <ul style="list-style-type: none"> <li>RFC 3246, <i>An Expedited Forwarding PHB (Per-Hop Behavior)</i>, defines one code point: <b>ef</b> (46).</li> <li>RFC 2597, <i>Assured Forwarding PHB Group</i>, defines 4 classes, with 3 drop precedences in each class, for a total of 12 code points:</li> </ul> <p><b>af11</b> (10), <b>af12</b> (12), <b>af13</b> (14),</p> <p><b>af21</b> (18), <b>af22</b> (20), <b>af23</b> (22),</p> <p><b>af31</b> (26), <b>af32</b> (28), <b>af33</b> (30),</p> <p><b>af41</b> (34), <b>af42</b> (36), <b>af43</b> (38)</p> |
| <b>ipv6-traffic-class-except</b> <i>number</i>     | Do not match the DSCP <b>number</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>ip-source-address</b> <i>address</i>            | (MX Series routers and EX Series switches only) IP address of the source node sending the packet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>learn-vlan-1p-priority</b> <i>number</i>        | <p>(MX Series routers, M320 router, and EX Series switches only) Match on the IEEE 802.1p learned VLAN priority bits in the provider VLAN tag (the only tag in a single-tag frame with 802.1Q VLAN tags or the outer tag in a dual-tag frame with 802.1Q VLAN tags). Specify a single value or multiple values from <b>0</b> through <b>7</b>.</p> <p>Compare with the <b>user-vlan-1p-priority</b> match condition.</p> <p><b>NOTE:</b> This match condition supports the presence of a control word for MX Series routers and the M320 router.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>learn-vlan-1p-priority-except</b> <i>number</i> | <p>(MX Series routers, M320 router, and EX Series switches only) Do not match on the IEEE 802.1p learned VLAN priority bits. For details, see the <b>learn-vlan-1p-priority</b> match condition.</p> <p><b>NOTE:</b> This match condition supports the presence of a control word for MX Series routers and the M320 router.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>learn-vlan-dei</b>                              | (MX Series routers and EX Series switches only) Match the user VLAN ID drop eligibility indicator (DEI) bit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>learn-vlan-dei-except</b>                       | (MX Series routers and EX Series switches only) Do not match the user VLAN ID DEI bit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>learn-vlan-id</b> <i>number</i>                 | (MX Series routers and EX Series switches only) VLAN identifier used for MAC learning.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>learn-vlan-id-except</b> <i>number</i>          | (MX Series routers and EX Series switches only) Do not match on the VLAN identifier used for MAC learning.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

Table 23: Firewall Filter Match Conditions for VPLS Traffic (*continued*)

| Match Condition                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>loss-priority level</b>        | <p>Packet loss priority (PLP) level. Specify a single level or multiple levels: <b>low</b>, <b>medium-low</b>, <b>medium-high</b>, or <b>high</b>.</p> <p>Supported on M120 and M320 routers; M7i and M10i routers with the Enhanced CFEB (CFEB-E); and MX Series routers.</p> <p>For IP traffic on M320, MX Series, and T Series routers with Enhanced II Flexible PIC Concentrators (FPCs) and EX Series switches, you must include the <b>tri-color</b> statement at the <b>[edit class-of-service]</b> hierarchy level to commit a PLP configuration with any of the four levels specified. If the <b>tri-color</b> statement is not enabled, you can only configure the <b>high</b> and <b>low</b> levels. This applies to all protocol families.</p> <p>For information about the <b>tri-color</b> statement and about using behavior aggregate (BA) classifiers to set the PLP level of incoming packets, see <i>Forwarding Classes Overview</i>.</p> |
| <b>loss-priority-except level</b> | <p>Do not match on the packet loss priority level. Specify a single level or multiple levels: <b>low</b>, <b>medium-low</b>, <b>medium-high</b>, or <b>high</b>.</p> <p>For information about using behavior aggregate (BA) classifiers to set the PLP level of incoming packets, see <i>Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>port number</b>                | (MX Series routers and EX Series switches only) TCP or UDP source or destination port. You cannot specify both the <b>port</b> match condition and either the <b>destination-port</b> or <b>source-port</b> match condition in the same term.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>port-except number</b>         | (MX Series routers and EX Series switches only) Do not match on the TCP or UDP source or destination port. You cannot specify both the <b>port</b> match condition and either the <b>destination-port</b> or <b>source-port</b> match condition in the same term.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>prefix-list name</b>           | <p>(MX Series routers and EX Series switches only) Match the destination or source prefixes in the specified list. Specify the name of a prefix list defined at the <b>[edit policy-options prefix-list prefix-list-name]</b> hierarchy level.</p> <p><b>NOTE:</b> VPLS prefix lists support only IPv4 addresses. IPv6 addresses included in a VPLS prefix list will be discarded.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>prefix-list name except</b>    | (MX Series routers and EX Series switches only) Do not match the destination or source prefixes in the specified list. For more information, see the <b>destination-prefix-list</b> match condition.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>source-mac-address address</b> | Source MAC address of a VPLS packet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>source-port number</b>         | (MX Series routers and EX Series switches only) TCP or UDP source port field. You cannot specify the <b>port</b> and <b>source-port</b> match conditions in the same term.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>source-port-except number</b>  | (MX Series routers and EX Series switches only) Do not match on the TCP or UDP source port field. You cannot specify the <b>port</b> and <b>source-port</b> match conditions in the same term.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>source-prefix-list name</b>    | <p>(MX Series routers and EX Series switches only) Match the source prefixes in the specified prefix list. Specify a prefix list name defined at the <b>[edit policy-options prefix-list prefix-list-name]</b> hierarchy level.</p> <p><b>NOTE:</b> VPLS prefix lists support only IPv4 addresses. IPv6 addresses included in a VPLS prefix list will be discarded.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

Table 23: Firewall Filter Match Conditions for VPLS Traffic (*continued*)

| Match Condition                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>source-prefix-list <i>name</i> except</b>      | (MX Series routers and EX Series switches only) Do not match the source prefixes in the specified prefix list. For more information, see the <b>source-prefix-list</b> match condition.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>tcp-flags <i>flags</i></b>                     | <p>Match one or more of the low-order 6 bits in the 8-bit TCP flags field in the TCP header.</p> <p>To specify individual bit fields, you can specify the following text synonyms or hexadecimal values:</p> <ul style="list-style-type: none"> <li>• <b>fin</b> (0x01)</li> <li>• <b>syn</b> (0x02)</li> <li>• <b>rst</b> (0x04)</li> <li>• <b>push</b> (0x08)</li> <li>• <b>ack</b> (0x10)</li> <li>• <b>urgent</b> (0x20)</li> </ul> <p>In a TCP session, the SYN flag is set only in the initial packet sent, while the ACK flag is set in all packets sent after the initial packet.</p> <p>You can string together multiple flags using the bit-field logical operators.</p> <p>If you configure this match condition for IPv6 traffic, we recommend that you also configure the <b>next-header tcp</b> match condition in the same term to specify that the TCP protocol is being used on the port.</p> |
| <b>traffic-type <i>type-name</i></b>              | (MX Series routers and EX Series switches only) Traffic type. Specify <b>broadcast</b> , <b>multicast</b> , <b>unknown-unicast</b> , or <b>known-unicast</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>traffic-type-except <i>type-name</i></b>       | (MX Series routers and EX Series switches only) Do not match on the traffic type. Specify <b>broadcast</b> , <b>multicast</b> , <b>unknown-unicast</b> , or <b>known-unicast</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>user-vlan-1p-priority <i>number</i></b>        | <p>(MX Series routers, M320 router, and EX Series switches only) Match on the IEEE 802.1p user priority bits in the customer VLAN tag (the inner tag in a dual-tag frame with 802.1Q VLAN tags). Specify a single value or multiple values from 0 through 7.</p> <p>Compare with the <b>learn-vlan-1p-priority</b> match condition.</p> <p><b>NOTE:</b> This match condition supports the presence of a control word for MX Series routers and the M320 router.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>user-vlan-1p-priority-except <i>number</i></b> | <p>(MX Series routers, M320 router, and EX Series switches only) Do not match on the IEEE 802.1p user priority bits. For details, see the <b>user-vlan-1p-priority</b> match condition.</p> <p><b>NOTE:</b> This match condition supports the presence of a control word for MX Series routers and the M320 router.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>user-vlan-id <i>number</i></b>                 | (MX Series routers and EX Series switches only) Match the first VLAN identifier that is part of the payload.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>user-vlan-id-except <i>number</i></b>          | (MX Series routers and EX Series switches only) Do not match on the first VLAN identifier that is part of the payload.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>vlan-ether-type <i>value</i></b>               | VLAN Ethernet type field of a VPLS packet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Table 23: Firewall Filter Match Conditions for VPLS Traffic (*continued*)

| Match Condition                           | Description                                                    |
|-------------------------------------------|----------------------------------------------------------------|
| <code>vlan-ether-type-except value</code> | Do not match on the VLAN Ethernet type field of a VPLS packet. |

- Related Documentation**
- *Guidelines for Configuring Firewall Filters*
  - *Firewall Filter Terminating Actions*
  - *Firewall Filter Nonterminating Actions*



# Monitoring and Tracing VPLS

- [Configuring Port Mirroring for VPLS Traffic on page 939](#)
- [Configuring Y.1731 Functionality for VPLS to Support Delay and Delay Variation on page 939](#)
- [Tracing VPLS Traffic and Operations on page 940](#)

## Configuring Port Mirroring for VPLS Traffic

---

You can configure port mirroring for VPLS traffic on the M7, M10i, M120, M320, and the MX Series routers. VPLS port mirroring is supported only M7i and M0i routers with the Enhanced Compact Forwarding Engine Board (CFEB-E). In addition, on M320 routers, VPLS port mirroring is supported only on Enhanced III Flexible PIC Concentrators (FPCs).

To configure port mirroring for VPLS include the **port-mirroring** statement at the **[edit forwarding-options]** hierarchy level. For more information about configuring port mirroring for VPLS for all platforms supported, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*. For information about configuring port mirroring for VPLS for MX Series routers, see the *Junos OS Layer 2 Switching and Bridging Library for Routing Devices*.

## Configuring Y.1731 Functionality for VPLS to Support Delay and Delay Variation

---

For VPLS, you can configure the Ethernet frame delay measurement (ETH-DM) functionality to trigger two-way ETH-DM and allow concurrent ETH-DM CLI sessions from the same local maintenance association end point (MEP). The feature also provides the option to perform ETH-DM for a given 802.1q priority, to set the size of the data type, length, and value (TLV), to disable the **session-id-tlv** option, and to generate XML output.

This feature complements the ITU-T Y.1731 Ethernet service OAM feature. On-demand delay measurement for VPLS is supported on MX Series routers installed with Rev-B DPCs. Only the two-way delay measurement feature is supported for VPLS connections.

MX Series routers with modular port concentrators (MPCs) and 10-Gigabit Ethernet MPCs with SFP+ support ITU-T Y.1731 functionality on VPLS for frame-delay and delay-variation.

This feature is currently supported only for up MEPs. Set the MEP direction to up by configuring the **up** option for the **direction** statement at the **[edit protocols oam ethernet**

**connectivity-fault-management maintenance-domain *md-name* maintenance-association *ma-name* mep *mep-id***] hierarchy level.

This feature also provides support for an optional configuration where you can delegate the server-side processing (for two-way delay measurement) to the Packet Forwarding Engine (PFE) to prevent overloading on the Routing Engine. To enable this feature, include the **delegate-server-processing** statement at the **[edit protocols oam ethernet connectivity-fault-management performance-monitoring]** hierarchy level. By default, the server-side processing is done by the Routing Engine.

The following commands enable you to monitor and maintain the Y.1731 feature for VPLS:

- To display the delay measurement values across a VPLS connection, use the **monitor ethernet delay-measurement two-way (*remote-mac-address* | *mep mep-id*) maintenance-domain *name* maintenance-association *name* count *count* wait *time* priority 802.1p-value *size* no-session-id-tlv xml** command.
- The feature also provides support for enhanced continuity measurement by using an existing continuity check protocol. The continuity for every remote MEP is measured as the percentage of time that a remote MEP was operationally up over the total administratively enabled time.

To display the continuity measurement information, use the **show oam ethernet connectivity-fault-management mep-database maintenance-domain *name* maintenance-association *name* local-mep *identifier* remote-mep *identifier*** command.

- You can restart the continuity measurement by clearing the currently measured operational uptime and administrative enabled time. To clear the existing continuity measurement and restart counting the operational uptime, use the **clear oam ethernet connectivity-fault-management continuity-measurement maintenance-domain *name* maintenance-association *name* local-mep *identifier* remote-mep *identifier*** command.
- To clear the delay statistics, issue a **clear oam ethernet connectivity-fault-management statistics** command or a **clear oam ethernet connectivity-fault-management delay-statistics two-way maintenance-domain *md-name* maintenance-association *ma-name*** command.

#### Related Documentation

- *Ethernet Interfaces Feature Guide for Routing Devices*
- *Configuring MEP Interfaces to Support Ethernet Frame Delay Measurements*
- *Example: Configuring Two-Way Ethernet Frame Delay Measurements with Single-Tagged Interfaces*

---

## Tracing VPLS Traffic and Operations

To trace VPLS traffic, include the **traceoptions** statement:

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

The following trace flags display the operations associated with VPLS:

- **all**—All VPLS tracing options
- **connections**—VPLS connections (events and state changes)
- **error**—Error conditions
- **nlri**—VPLS advertisements received or sent using BGP
- **route**—Trace-routing information
- **topology**—VPLS topology changes caused by reconsideration or advertisements received from other PE routers using BGP



## PART 8

# Connecting Layer 2 VPNs and Circuits to Other VPNs

- [Connecting Layer 2 VPNs to Other VPNs on page 945](#)
- [Connecting Layer 2 Circuits to Other VPNs on page 989](#)



# Connecting Layer 2 VPNs to Other VPNs

- [Layer 2 VPN to Layer 2 VPN Connections on page 945](#)
- [Using the Layer 2 Interworking Interface to Interconnect a Layer 2 VPN to a Layer 2 VPN on page 945](#)
- [Example: Interconnecting a Layer 2 VPN with a Layer 2 VPN on page 947](#)
- [Interconnecting Layer 2 VPNs with Layer 3 VPNs Overview on page 963](#)
- [Example: Interconnecting a Layer 2 VPN with a Layer 3 VPN on page 964](#)

## Layer 2 VPN to Layer 2 VPN Connections

---

As the need to link different Layer 2 services to one another for expanded service offerings grows, Layer 2 MPLS VPN services are increasingly in demand. Junos OS enables you to terminate Layer 2 VPN into Layer 2 VPN (also known as Layer 2 VPN stitching) using the Layer 2 interworking (iw0) interface.

Another way to do this is to use a Tunnel Services PIC to loop packets out and back from the Packet Forwarding Engine (PFE), to link together Layer 2 networks. The Layer 2 interworking software interface avoids the need for the Tunnel Services PIC and overcomes the limitation of bandwidth constraints imposed by the Tunnel Services PIC.

### Related Documentation

- [Example: Interconnecting a Layer 2 VPN with a Layer 2 VPN on page 947](#)

## Using the Layer 2 Interworking Interface to Interconnect a Layer 2 VPN to a Layer 2 VPN

---

Instead of using a physical Tunnel PIC for looping the packet received from the Layer 2 VPN to another Layer 2 VPN, the Layer 2 Interworking interface uses Junos OS to stitch together both Layer 2 VPN routes.

To configure the interworking interface, include the **iw0** statement. The **iw0** statement is configured at the **[edit interfaces]** hierarchy level.

```
[edit interfaces]
iw0 {
 unit 0 {
 peer 1;
 }
}
```

```

unit 1 {
 peer 0;
}

```



**NOTE:** You must always create and delete (or deactivate) interworking (iw) interfaces in pairs, such as:

```

set interfaces iw0 unit 0 peer-unit 1
set interfaces iw0 unit 1 peer-unit 0

```

An error message displays if you delete or deactivate only one of the interworking interfaces. To successfully deactivate the interfaces and avoid any configuration errors, you must deactivate both.

The configuration of an interworking (iw) interface is similar to the configuration of a logical tunnel (lt) interface. In this example, the logical interfaces must be associated with the endpoints of both Layer 2 VPN connections terminating on this router. To make the association, include the **interfaces** statement and specify **iw0** as the interface name. Include the statement at the **[edit routing-instances routing-instances-name protocols l2vpn site site-name]** hierarchy level for each routing instance. The **routing-instances** statement is configured at the **[edit routing-instances]** hierarchy level.

```

[edit routing-instances]
L2VPN-PE1 {
 instance-type l2vpn;
 interface iw0.0;
 route-distinguisher 65000:3;
 vrf-target target:65000:2;
 protocols {
 l2vpn {
 encapsulation-type ethernet;
 site CE3 {
 site-identifier 3;
 interface iw0.0 {
 remote-site-id 1;
 }
 }
 }
 }
}
L2VPN-PE5 {
 instance-type l2vpn;
 interface iw0.1;
 route-distinguisher 65000:33;
 vrf-target target:65000:2;
 protocols {
 l2vpn {
 encapsulation-type ethernet;
 site CE3 {
 site-identifier 3;
 interface iw0.1 {
 remote-site-id 5;
 }
 }
 }
 }
}

```

```

 }
 }
}

```

In addition to the **iw0** interface configuration, Layer 2 interworking **l2iw** protocols need to be configured. Without the **l2iw** configuration, the **l2iw** routes will not be formed, regardless of whether any **iw** interfaces are present. Only standard trace options can be configured within the **l2iw** protocol. The minimum configuration necessary for the feature to work is shown below:

```

[edit]
protocols {
 l2iw;
}

```

#### Related Documentation

- [Understanding Layer 2 VPNs on page 121](#)
- [Layer 2 VPN Applications on page 122](#)
- [Example: Interconnecting a Layer 2 VPN with a Layer 2 VPN on page 947](#)

## Example: Interconnecting a Layer 2 VPN with a Layer 2 VPN

This example provides a step-by-step procedure for interconnecting and verifying a Layer 2 VPN with a Layer 2 VPN. It contains the following sections:

- [Requirements on page 947](#)
- [Overview and Topology on page 947](#)
- [Configuration on page 948](#)

### Requirements

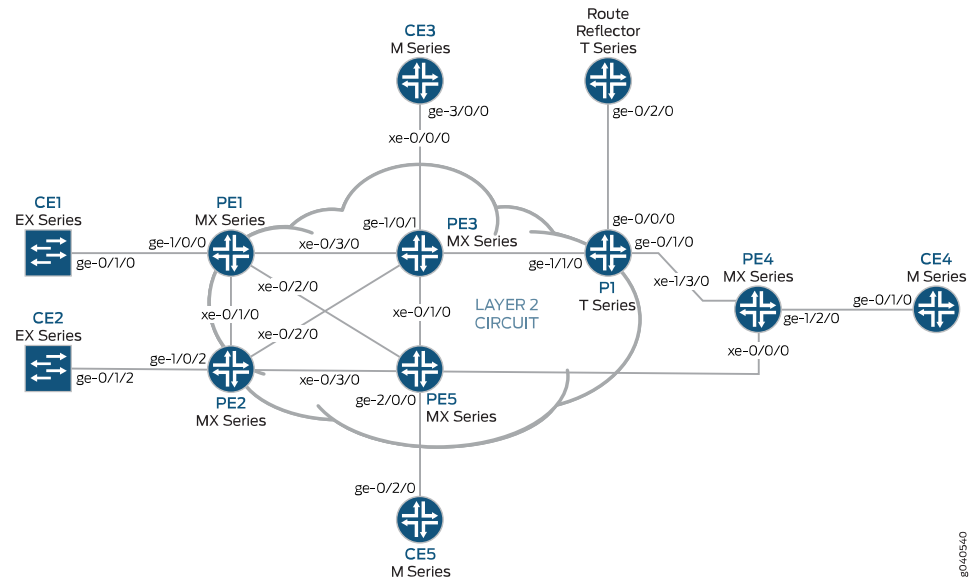
This example uses the following hardware and software components:

- Junos OS Release 9.3 or later
- 2 MX Series 3D Universal Edge Routers
- 2 M Series Multiservice Edge Routers
- 1 T Series Core Routers
- 1 EX Series Ethernet Switches

### Overview and Topology

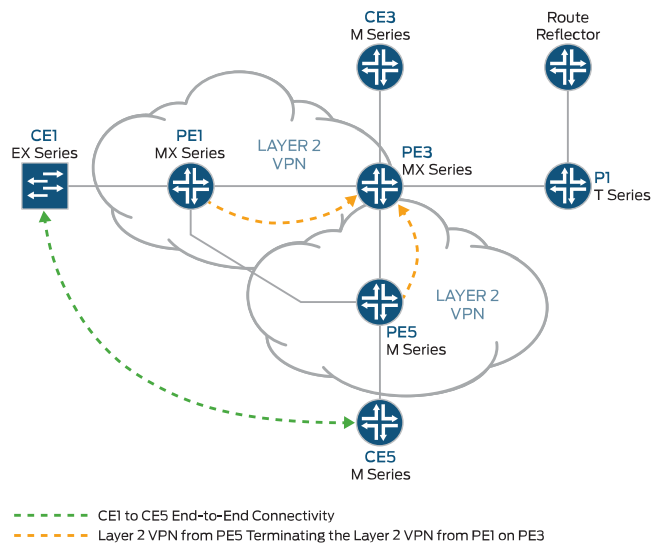
The physical topology of the Layer 2 VPN to Layer 2 VPN connection example is shown in [Figure 81 on page 948](#).

Figure 81: Physical Topology of a Layer 2 VPN to Layer 2 VPN Connection



The logical topology of a Layer 2 VPN to Layer 2 VPN connection is shown in [Figure 82 on page 948](#).

Figure 82: Logical Topology of a Layer 2 VPN to Layer 2 VPN Connection



## Configuration



**NOTE:** In any configuration session, it is good practice to verify periodically 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
- **CE3** identifies the customer edge 3 (CE3) router
- **PE3** identifies the provider edge 3 (PE3) router
- **CE5** identifies the customer edge 5 (CE5) router
- **PE5** identifies the provider edge 5 (PE5) router

This example is organized in the following sections:

- [Configuring Protocols on the PE and P Routers on page 949](#)
- [Verifying the Layer 2 VPN to Layer 2 VPN Connection on Router PE3 on page 954](#)
- [Verifying the Layer 2 VPN to Layer 2 VPN Connection on Router PE3 on page 956](#)
- [Results on page 958](#)

### Configuring Protocols on the PE and P Routers

#### Step-by-Step Procedure

All of the PE routers and P routers are configured with OSPF as the IGP protocol. The MPLS, LDP, and BGP protocols are enabled on all of the interfaces except **fxp0.0**. Core-facing interfaces are enabled with the MPLS address and inet address.

1. Configure all the PE and P routers with OSPF as the IGP. Enable the MPLS, LDP, and BGP protocols on all interfaces except **fxp0.0**. The following configuration snippet shows the protocol configuration for Router PE1:

```
[edit]
protocols {
 mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 bgp {
 group RR {
 type internal;
 local-address 192.0.2.1;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 }
}
```

```

 }
 }
}
ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
}
}

```

2. Configure the PE and P routers with OSPF as the IGP. Enable the MPLS, LDP, and BGP protocols on all interfaces except **fxp0.0**. The following configuration snippet shows the protocol configuration for Router PE3:

```

[edit]
protocols {
 mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 bgp {
 group RR {
 type internal;
 local-address 192.0.2.3;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 }
 ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}

```

### Step-by-Step Procedure

#### Configuring the Layer 2 VPN Protocol and Interfaces

1. On Router PE1, configure the **ge-1/0/0** interface encapsulation. To configure the interface encapsulation, include the **encapsulation** statement and specify the **ethernet-ccc** option (vlan-ccc encapsulation is also supported). Configure the

**ge-1/0/0.0** logical interface family for circuit cross-connect functionality. To configure the logical interface family, include the **family** statement and specify the **ccc** option. The encapsulation should be configured the same way for all routers in the Layer 2 VPN domain.

```
[edit interfaces]
ge-1/0/0 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.1/24;
 }
 }
}
```

2. On Router PE1, configure the Layer 2 VPN protocols. Configure the remote site ID as 3. Site ID 3 represents Router PE3 (Hub-PE). To configure the Layer 2 VPN protocols, include the **l2vpn** statement at the **[edit routing-instances routing-instances-name protocols]** hierarchy level. Layer 2 VPNs use BGP as the signaling protocol.

```
[edit routing-instances]
L2VPN {
 instance-type l2vpn;
 interface ge-1/0/0.0;
 route-distinguisher 65000:1;
 vrf-target target:65000:2;
 protocols {
 l2vpn {
 encapsulation-type ethernet;
 site CE1 {
 site-identifier 1;
 interface ge-1/0/0.0 {
 remote-site-id 3;
 }
 }
 }
 }
}
```

3. On Router PE5, configure the **ge-2/0/0** interface encapsulation by including the **encapsulation** statement and specify the **ethernet-ccc** option. Configure the **ge-1/0/0.0** logical interface family for circuit cross-connect functionality by including the **family** statement and specifying the **ccc** option.

```
[edit interfaces]
ge-2/0/0 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
}
```

```

}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.5/24;
 }
 }
}

```

4. On Router PE5, configure the Layer 2 VPN protocols by including the **l2vpn** statement at the **[edit routing-instances *routing-instances-name* protocols]** hierarchy level. Configure the remote site ID as **3**.

```

[edit routing-instances]
L2VPN {
 instance-type l2vpn;
 interface ge-2/0/0.0;
 route-distinguisher 65000:5;
 vrf-target target:65000:2;
 protocols {
 l2vpn {
 encapsulation-type ethernet;
 site CE5 {
 site-identifier 5;
 interface ge-2/0/0.0 {
 remote-site-id 3;
 }
 }
 }
 }
}

```

5. On Router PE3, configure the **iw0** interface with two logical interfaces. To configure the **iw0** interface, include the **interfaces** statement and specify **iw0** as the interface name. For the unit 0 logical interface, include the **peer-unit** statement and specify the logical interface **unit 1** as the peer interface. For the unit 1 logical interface, include the **peer-unit** statement and specify the logical interface **unit 0** as the peer interface.

```

[edit interfaces]
iw0 {
 unit 0 {
 encapsulation ethernet-ccc;
 peer-unit 1;
 }
 unit 1 {
 encapsulation ethernet-ccc;
 peer-unit 0;
 }
}

```

6. On Router PE3, configure the edge-facing **ge-1/0/1** interface encapsulation by including the **encapsulation** statement and specifying the **ethernet-ccc** option.

```

[edit interfaces]
ge-1/0/1 {
 encapsulation ethernet-ccc;
 unit 0 {

```

```

 family ccc;
 }
}

```

7. On Router PE3, configure the logical loopback interface. The loopback interface is used to establish the targeted LDP sessions to Routers PE1 and Router PE5.

```

[edit interfaces]
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.3/24;
 }
 }
}

```

8. On Router PE3, enable the Layer 2 interworking protocol. To enable the Layer 2 interworking protocol, include the **l2iw** statement at the **[edit protocols]** hierarchy level.

```

[edit protocols]
l2iw;

```

9. On Router PE3, configure two Layer 2 VPN routing instances to terminate the Layer 2 VPN virtual circuits from Router PE1 and Router PE5, as shown.

```

[edit routing-instances]
L2VPN-PE1 {
 instance-type l2vpn;
 interface iw0.0;
 route-distinguisher 65000:3;
 vrf-target target:65000:2;
 protocols {
 l2vpn {
 encapsulation-type ethernet;
 site CE3 {
 site-identifier 3;
 interface iw0.0 {
 remote-site-id 1;
 }
 }
 }
 }
}
L2VPN-PE5 {
 instance-type l2vpn;
 interface iw0.1;
 route-distinguisher 65000:33;
 vrf-target target:65000:2;
 protocols {
 l2vpn {
 encapsulation-type ethernet;
 site CE3 {
 site-identifier 3;
 interface iw0.1 {
 remote-site-id 5;
 }
 }
 }
 }
}

```

```

 }
 }
}

```

### Verifying the Layer 2 VPN to Layer 2 VPN Connection on Router PE3

- Step-by-Step Procedure**
1. BGP is used for control plane signaling in a Layer 2 VPN. On Router PE1, use the **show bgp** command to verify that the BGP control plane for the Layer 2 VPN, has established a neighbor relationship with the route reflector that has IP address **192.0.2.7**.

Three Layer 2 VPN routes are received from the route reflector for each PE router in the topology.

```
user@PE1> show bgp summary
```

```
Groups: 1 Peers: 1 Down peers: 0
```

| Table                                     | Tot Paths | Act Paths | Suppressed | History | Damp  | State       | Pending |
|-------------------------------------------|-----------|-----------|------------|---------|-------|-------------|---------|
| bgp.l2vpn.0                               | 3         | 3         | 0          | 0       | 0     | 0           | 0       |
| Peer                                      | AS        | InPkt     | OutPkt     | OutQ    | Flaps | Last Up/Dwn |         |
| State #Active/Received/Accepted/Damped... |           |           |            |         |       |             |         |
| 192.0.2.7                                 | 65000     | 190       | 192        | 0       | 0     | 1:24:40     | Establ  |
| bgp.l2vpn.0: 3/3/3/0                      |           |           |            |         |       |             |         |
| L2VPN.l2vpn.0: 3/3/3/0                    |           |           |            |         |       |             |         |

2. On Router PE1, use the **show route** command to verify that the BGP Layer 2 VPN routes are stored in the **L2VPN.l2vpn.0** routing table for each PE router.

```
user@PE1> show route table L2VPN.l2vpn.0
```

```
L2VPN.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
```

```
65000:1:1:3/96
 *[L2VPN/170/-101] 01:31:53, metric2 1
 Indirect
65000:3:3:1/96
 *[BGP/170] 01:24:58, localpref 100, from 192.0.2.7
 AS path: I
 > to 10.10.1.2 via xe-0/3/0.0
65000:5:5:3/96
 *[BGP/170] 01:24:58, localpref 100, from 192.0.2.7
 AS path: I
 > to 10.10.3.2 via xe-0/2/0.0
65000:33:3:5/96
 *[BGP/170] 01:24:58, localpref 100, from 192.0.2.7
 AS path: I
 > to 10.10.1.2 via xe-0/3/0.0
```

3. On Router PE1, use the **show ldp session** command to verify that targeted LDP sessions are established to the PE routers in the network and that the state is **Operational**.

```
user@PE1> show ldp session
```

| Address   | State       | Connection | Hold time |
|-----------|-------------|------------|-----------|
| 192.0.2.2 | Operational | Open       | 24        |
| 192.0.2.3 | Operational | Open       | 22        |
| 192.0.2.5 | Operational | Open       | 28        |

4. On Router PE1, use the **show l2vpn connections** command to verify that the Layer 2 VPN to site 3 on Router PE3 (Hub-PE) is **Up**.

```
user@PE1> show l2vpn connections
```

Layer-2 VPN connections:

Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -> -- only outbound connection is up           |
| CN -- circuit not provisioned    | <- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unknown connection status  | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not available              |
| BK -- Backup connection          | ST -- Standby connection                       |
| PF -- Profile parse failure      | PB -- Profile busy                             |

Legend for interface status

Up -- operational  
Dn -- down

Instance: L2VPN

Local site: CE1 (1)

| connection-site                                                  | Type | St | Time last up        | # Up trans |
|------------------------------------------------------------------|------|----|---------------------|------------|
| 3                                                                | rmt  | Up | Jan 5 18:08:25 2010 | 1          |
| Remote PE: 192.0.2.3, Negotiated control-word: Yes (Null)        |      |    |                     |            |
| Incoming label: 800000, Outgoing label: 800000                   |      |    |                     |            |
| Local interface: ge-1/0/0.0, Status: Up, Encapsulation: ETHERNET |      |    |                     |            |
| 5                                                                | rmt  | OR |                     |            |

5. On Router PE1, use the **show route** command to verify that the **mpls.0** routing table is populated with the Layer 2 VPN routes used to forward the traffic using an LDP label. Notice that in this example, the router is pushing label **8000000**.

```
user@PE1> show route table mpls.0
```

```
[edit]
```

```
mpls.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
```

```
+ = Active Route, - = Last Active, * = Both
```

```

0 *[MPLS/0] 1w1d 11:36:44, metric 1
 Receive
1 *[MPLS/0] 1w1d 11:36:44, metric 1
 Receive
2 *[MPLS/0] 1w1d 11:36:44, metric 1
 Receive
300432 *[LDP/9] 3d 04:25:02, metric 1
 > to 10.10.2.2 via xe-0/1/0.0, Pop
300432(S=0) *[LDP/9] 3d 04:25:02, metric 1
 > to 10.10.2.2 via xe-0/1/0.0, Pop
300768 *[LDP/9] 3d 04:25:02, metric 1
 > to 10.10.3.2 via xe-0/2/0.0, Pop
300768(S=0) *[LDP/9] 3d 04:25:02, metric 1
 > to 10.10.3.2 via xe-0/2/0.0, Pop

```

```

300912 *[LDP/9] 3d 04:25:02, metric 1
 > to 10.10.3.2 via xe-0/2/0.0, Swap 299856
301264 *[LDP/9] 3d 04:24:58, metric 1
 > to 10.10.1.2 via xe-0/3/0.0, Swap 308224
301312 *[LDP/9] 3d 04:25:01, metric 1
 > to 10.10.1.2 via xe-0/3/0.0, Pop
301312(S=0) *[LDP/9] 3d 04:25:01, metric 1
 > to 10.10.1.2 via xe-0/3/0.0, Pop
800000 *[L2VPN/7] 01:25:28
 > via ge-1/0/0.0, Pop Offset: 4
ge-1/0/0.0 *[L2VPN/7] 01:25:28, metric 21
 > to 10.10.1.2 via xe-0/3/0.0, Push 800000 Offset: -4

```

### Verifying the Layer 2 VPN to Layer 2 VPN Connection on Router PE3

- Step-by-Step Procedure**
1. On Router PE3, use the **show l2vpn connections** command to verify that the Layer 2 VPN connections from Router PE1 and Router PE5 are **Up** and are using the **iw0** interface.

```
user@PE3> show l2vpn connections
```

```
Instance: L2VPN-PE1
```

```
Local site: CE3 (3)
```

| connection-site                                             | Type | St | Time last up        | # Up trans |
|-------------------------------------------------------------|------|----|---------------------|------------|
| 1                                                           | rmt  | Up | Jan 5 18:08:22 2010 | 1          |
| Remote PE: 192.0.2.1, Negotiated control-word: Yes (Null)   |      |    |                     |            |
| Incoming label: 800000, Outgoing label: 800000              |      |    |                     |            |
| Local interface: iw0.0, Status: Up, Encapsulation: ETHERNET |      |    |                     |            |
| 5                                                           | rmt  | OR |                     |            |

```
Instance: L2VPN-PE5
```

```
Local site: CE3 (3)
```

| connection-site                                             | Type | St | Time last up        | # Up trans |
|-------------------------------------------------------------|------|----|---------------------|------------|
| 1                                                           | rmt  | CN |                     |            |
| 5                                                           | rmt  | Up | Jan 5 18:08:22 2010 | 1          |
| Remote PE: 192.0.2.5, Negotiated control-word: Yes (Null)   |      |    |                     |            |
| Incoming label: 800002, Outgoing label: 800000              |      |    |                     |            |
| Local interface: iw0.1, Status: Up, Encapsulation: ETHERNET |      |    |                     |            |

2. On Router PE3, use the **show ldp neighbor** command to verify that the targeted LDP session neighbor IP addresses are shown.

```
user@PE3> show ldp neighbor
```

| Address   | Interface | Label space ID | Hold time |
|-----------|-----------|----------------|-----------|
| 192.0.2.1 | lo0.0     | 192.0.2.1:0    | 44        |
| 192.0.2.2 | lo0.0     | 192.0.2.2:0    | 42        |
| 192.0.2.4 | lo0.0     | 192.0.2.4:0    | 31        |
| 192.0.2.5 | lo0.0     | 192.0.2.5:0    | 44        |

3. On Router PE3, use the **show bgp summary** command to verify that the BGP control plane for the Layer 2 VPN, has established a neighbor relationship with the route reflector that has IP address **192.0.2.7**.

```
user@PE3> show bgp summary
```

```
Groups: 1 Peers: 1 Down peers: 0
```

| Table                                     | Tot Paths | Act Paths | Suppressed | History | Damp  | State       | Pending |
|-------------------------------------------|-----------|-----------|------------|---------|-------|-------------|---------|
| bgp.l2vpn.0                               | 2         | 2         | 0          | 0       | 0     | 0           | 0       |
| Peer                                      | AS        | InPkt     | OutPkt     | OutQ    | Flaps | Last Up/Dwn |         |
| State #Active/Received/Accepted/Damped... |           |           |            |         |       |             |         |
| 192.0.2.7                                 | 65000     | 10092     | 10195      | 0       | 0     | 3d 4:23:27  | Establ  |
| bgp.l2vpn.0: 2/2/2/0                      |           |           |            |         |       |             |         |



L2VPN-PE1.l2vpn.0: 2/2/2/0

L2VPN-PE5.l2vpn.0: 2/2/2/0

4. On Router PE3, use the **show ldp session** command to verify that targeted LDP sessions are established to all of the PE routers in the network and that the state is **Operational**.

```
user@PE3> show ldp session
Address State Connection Hold time
192.0.2.1 Operational Open 24
192.0.2.2 Operational Open 22
192.0.2.4 Operational Open 20
192.0.2.5 Operational Open 24
```

5. On Router PE3, use the **show route** command to verify that the **mpls.0** routing table is populated with the Layer 2 VPN routes used to forward the traffic using an LDP label. Notice that in this example, the router is swapping label **800000**. Also notice the two **iw0** interfaces that are used for the Layer 2 interworking routes.

```
user@PE3> show route table mpls.0
mpls.0: 16 destinations, 18 routes (16 active, 2 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0 *[MPLS/0] 1w1d 11:50:14, metric 1
 Receive
1 *[MPLS/0] 1w1d 11:50:14, metric 1
 Receive
2 *[MPLS/0] 1w1d 11:50:14, metric 1
 Receive
308160 *[LDP/9] 3d 04:38:45, metric 1
 > to 10.10.1.1 via xe-0/3/0.0, Pop
308160(S=0) *[LDP/9] 3d 04:38:45, metric 1
 > to 10.10.1.1 via xe-0/3/0.0, Pop
308176 *[LDP/9] 3d 04:38:44, metric 1
 > to 10.10.6.2 via xe-0/1/0.0, Pop
308176(S=0) *[LDP/9] 3d 04:38:44, metric 1
 > to 10.10.6.2 via xe-0/1/0.0, Pop
308192 *[LDP/9] 00:07:18, metric 1
 > to 10.10.20.1 via xe-0/0/0.0, Swap 601649
 > to 10.10.6.2 via xe-0/1/0.0, Swap 299856
308208 *[LDP/9] 3d 04:38:44, metric 1
 > to 10.10.5.1 via xe-0/2/0.0, Pop
308208(S=0) *[LDP/9] 3d 04:38:44, metric 1
 > to 10.10.5.1 via xe-0/2/0.0, Pop
308224 *[LDP/9] 3d 04:38:42, metric 1
 > to 10.10.20.1 via xe-0/0/0.0, Pop
308224(S=0) *[LDP/9] 3d 04:38:42, metric 1
 > to 10.10.20.1 via xe-0/0/0.0, Pop
800000 *[L2IW/6] 01:39:13, metric 21
 > to 10.10.6.2 via xe-0/1/0.0, Swap 800000
 [L2VPN/7] 01:39:13
 > via iw0.0, Pop Offset: 4
800002 *[L2IW/6] 01:39:13, metric 21
 > to 10.10.1.1 via xe-0/3/0.0, Swap 800000
 [L2VPN/7] 01:39:13
 > via iw0.1, Pop Offset: 4
iw0.0 *[L2VPN/7] 01:39:13, metric 21
 > to 10.10.1.1 via xe-0/3/0.0, Push 800000 Offset: -4
```

```
iw0.1 *[L2VPN/7] 01:39:13, metric2 1
> to 10.10.6.2 via xe-0/1/0.0, Push 800000 Offset: -4
```

### Step-by-Step Procedure Testing Layer 2 VPN to Layer 2 VPN Connectivity (CE1 to CE5)

1. On Router CE1, use the **ping** command to test connectivity to Router CE5. Notice that the response time is in milliseconds, confirming that the ping response is returned.

```
user@CE1>ping 198.51.100.11
PING 198.51.100.11 (198.51.100.11): 56 data bytes
64 bytes from 198.51.100.11: icmp_seq=1 ttl=64 time=22.425 ms
64 bytes from 198.51.100.11: icmp_seq=2 ttl=64 time=1.299 ms
64 bytes from 198.51.100.11: icmp_seq=3 ttl=64 time=1.032 ms
64 bytes from 198.51.100.11: icmp_seq=4 ttl=64 time=1.029 ms
```

2. On Router CE5, use the **ping** command to test connectivity to Router CE1. Notice that the response time is in milliseconds, confirming that the ping response is returned.

```
user@CE5>ping 198.51.100.1
PING 198.51.100.1 (198.51.100.1): 56 data bytes
64 bytes from 198.51.100.1: icmp_seq=0 ttl=64 time=1.077 ms
64 bytes from 198.51.100.1: icmp_seq=1 ttl=64 time=0.957 ms
64 bytes from 198.51.100.1: icmp_seq=2 ttl=64 time=1.057 ms 1.017 ms
```

## Results

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

The relevant sample configuration for Router PE1 follows.

```
Router PE1 chassis {
 dump-on-panic;
 fpc 1 {
 pic 3 {
 tunnel-services {
 bandwidth 1g;
 }
 }
 }
 network-services ethernet;
 }
 interfaces {
 xe-0/1/0 {
 unit 0 {
 family inet {
 address 10.10.2.1/30;
 }
 family mpls;
 }
 }
 xe-0/2/0 {
 unit 0 {
 family inet {
 address 10.10.3.1/30;
 }
 }
 }
 }
```

```

 }
 family mpls;
 }
}
xe-0/3/0 {
 unit 0 {
 family inet {
 address 10.10.1.1/30;
 }
 family mpls;
 }
}
ge-1/0/0 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.1/24;
 }
 }
}
}
routing-options {
 static {
 route 172.16.0.0/8 next-hop 172.19.59.1;
 }
 autonomous-system 65000;
}
protocols {
 mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}
bgp {
 group RR {
 type internal;
 local-address 192.0.2.1;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
}
ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}

```

```

 }
 }
 ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}
routing-instances {
 L2VPN {
 instance-type l2vpn;
 interface ge-1/0/0.0;
 route-distinguisher 65000:1;
 vrf-target target:65000:2;
 protocols {
 l2vpn {
 encapsulation-type ethernet;
 site CE1 {
 site-identifier 1;
 interface ge-1/0/0.0 {
 remote-site-id 3;
 }
 }
 }
 }
 }
}
}

```

The relevant sample configuration for Router PE3 follows.

```

Router PE3 chassis {
 dump-on-panic;
 fpc 1 {
 pic 3 {
 tunnel-services {
 bandwidth 1g;
 }
 }
 }
 network-services ethernet;
 }
 interfaces {
 xe-0/0/0 {
 unit 0 {
 family inet {
 address 10.10.20.2/30;
 }
 family mpls;
 }
 }
 xe-0/1/0 {
 unit 0 {
 family inet {
 address 10.10.6.1/30;
 }
 }
 }
 }

```

```

 family mpls;
 }
}
xe-0/2/0 {
 unit 0 {
 family inet {
 address 10.10.5.2/30;
 }
 family mpls;
 }
}
xe-0/3/0 {
 unit 0 {
 family inet {
 address 10.10.1.2/30;
 }
 family mpls;
 }
}
ge-1/0/1 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
}
iw0 {
 unit 0 {
 encapsulation ethernet-ccc;
 peer-unit 1;
 }
 unit 1 {
 encapsulation ethernet-ccc;
 peer-unit 0;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.3/24;
 }
 }
}
}
routing-options {
 static {
 route 172.16.0.0/8 next-hop 172.19.59.1;
 }
 autonomous-system 65000;
}
protocols {
 l2iw;
 mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}

```

```
}
bgp {
 group RR {
 type internal;
 local-address 192.0.2.3;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
}
ospf {
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}
ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
}
}
routing-instances {
 L2VPN-PE1 {
 instance-type l2vpn;
 interface iw0.0;
 route-distinguisher 65000:3;
 vrf-target target:65000:2;
 protocols {
 l2vpn {
 encapsulation-type ethernet;
 site CE3 {
 site-identifier 3;
 interface iw0.0 {
 remote-site-id 1;
 }
 }
 }
 }
 }
 L2VPN-PE5 {
 instance-type l2vpn;
 interface iw0.1;
 route-distinguisher 65000:33;
 vrf-target target:65000:2;
 protocols {
 l2vpn {
 encapsulation-type ethernet;
 site CE3 {
 site-identifier 3;
 interface iw0.1 {
 remote-site-id 5;
 }
 }
 }
 }
 }
}
```

```

 }
 }
}

```

#### Related Documentation

- [Understanding Layer 2 VPNs on page 121](#)
- [Layer 2 VPN Applications on page 122](#)
- [Using the Layer 2 Interworking Interface to Interconnect a Layer 2 VPN to a Layer 2 VPN on page 945](#)

## Interconnecting Layer 2 VPNs with Layer 3 VPNs Overview

As MPLS-based Layer 2 services grow in demand, new challenges arise for service providers to be able to interoperate with Layer 2 and Layer 3 services and give their customers value-added services. Junos OS has various features to address the needs of service providers. One of these features is the use of a logical tunnel interface. This Junos OS functionality makes use of a tunnel PIC to loop packets out and back from the Packet Forwarding Engine to link the Layer 2 network with the Layer 3 network. The solution is limited by the logical tunnel bandwidth constraints imposed by the tunnel PIC.

### Interconnecting Layer 2 VPNs with Layer 3 VPNs Applications

Interconnecting a Layer 2 VPN with a Layer 3 VPN provides the following benefits:

- **A single access line to provide multiple services**—Traditional VPNs over Layer 2 circuits require the provisioning and maintenance of separate networks for IP and for VPN services. In contrast, Layer 2 VPNs enable the sharing of a provider's core network infrastructure between IP and Layer 2 VPN services, thereby reducing the cost of providing those services.
- **Flexibility**—Many different types of networks can be accommodated by the service provider. If all sites in a VPN are owned by the same enterprise, this is an intranet. If various sites are owned by different enterprises, the VPN is an extranet. A site can be located in more than one VPN.
- **Wide range of possible policies**—You can give every site in a VPN a different route to every other site, or you can force traffic between certain pairs of sites routed via a third site and so pass certain traffic through a firewall.
- **Scalable network**—This design enhances the scalability because it eliminates the need for provider edge (PE) routers to maintain all of the service provider's VPN routes. Each PE router maintains a VRF table for each of its directly connected sites. Each customer connection (such as a Frame Relay PVC, an ATM PVC, or a VLAN) is mapped to a specific VRF table. Thus, it is a port on the PE router and not a site that is associated with a VRF table. Multiple ports on a PE router can be associated with a single VRF table. It is the ability of PE routers to maintain multiple forwarding tables that supports the per-VPN segregation of routing information.

- Use of route reflectors—Provider edge routers can maintain IBGP sessions to route reflectors as an alternative to a full mesh of IBGP sessions. Deploying multiple route reflectors enhances the scalability of the RFC 2547bis model because it eliminates the need for any single network component to maintain all VPN routes.
- Multiple VPNs are kept separate and distinct from each other—The customer edge routers do not peer with each other. Two sites have IP connectivity over the common backbone only, and only if there is a VPN which contains both sites. This feature keeps the VPNs separate and distinct from each other, even if two VPNs have an overlapping address space.
- Simple for customers to use—Customers can obtain IP backbone services from a service provider, and they do not need to maintain their own backbones.

**Related  
Documentation**

- [Understanding Layer 3 VPNs](#)
- [Example: Interconnecting a Layer 2 VPN with a Layer 3 VPN on page 964](#)

---

## Example: Interconnecting a Layer 2 VPN with a Layer 3 VPN

This example provides a step-by-step procedure and commands for interconnecting and verifying a Layer 2 VPN with a Layer 3 VPN. It contains the following sections:

- [Requirements on page 964](#)
- [Overview and Topology on page 964](#)
- [Configuration on page 967](#)
- [Verification on page 982](#)

### Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.3 or later
- Five MX Series routers
- Three M Series routers
- Two T Series routers

### Overview and Topology

A Layer 2 VPN is a type of virtual private network (VPN) that uses MPLS labels to transport data. The communication occurs between the provider edge (PE) routers.

Layer 2 VPNs use BGP as the signaling protocol and, consequently, have a simpler design and require less provisioning overhead than traditional VPNs over Layer 2 circuits. BGP signaling also enables autodiscovery of Layer 2 VPN peers. Layer 2 VPNs can have either a full-mesh or a hub-and-spoke topology. The tunneling mechanism in the core network is, typically, MPLS. However, Layer 2 VPNs can also use other tunneling protocols, such as GRE.



Layer 3 VPNs are based on RFC 2547bis, *BGP/MPLS IP VPNs*. RFC 2547bis defines a mechanism by which service providers can use their IP backbones to provide VPN services to their customers. A Layer 3 VPN is a set of sites that share common routing information and whose connectivity is controlled by a collection of policies. The sites that make up a Layer 3 VPN are connected over a provider's existing public Internet backbone. RFC 2547bis VPNs are also known as BGP/MPLS VPNs because BGP is used to distribute VPN routing information across the provider's backbone, and MPLS is used to forward VPN traffic across the backbone to remote VPN sites.

Customer networks, because they are private, can use either public addresses or private addresses, as defined in RFC 1918, *Address Allocation for Private Internets*. When customer networks that use private addresses connect to the public Internet infrastructure, the private addresses might overlap with the same private addresses used by other network users. MPLS/BGP VPNs solve this problem by adding a *route distinguisher*. A route distinguisher is a VPN identifier prefix that is added to each address from a particular VPN site, thereby creating an address that is unique both within the VPN and within the Internet.

In addition, each VPN has its own VPN-specific routing table that contains the routing information for that VPN only. To separate a VPN's routes from routes in the public Internet or those in other VPNs, the PE router creates a separate routing table for each VPN called a VPN routing and forwarding (VRF) table. The PE router creates one VRF table for each VPN that has a connection to a customer edge (CE) router. Any customer or site that belongs to the VPN can access only the routes in the VRF tables for that VPN. Every VRF table has one or more extended community attributes associated with it that identify the route as belonging to a specific collection of routers. One of these, the *route target* attribute, identifies a collection of sites (VRF tables) to which a PE router distributes routes. The PE router uses the route target to constrain the import of remote routes into its VRF tables.

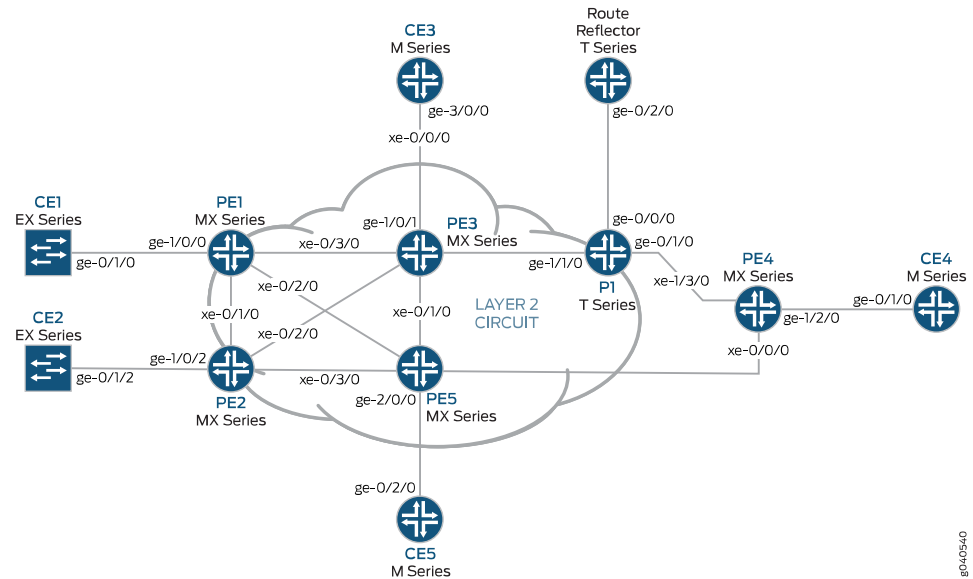
When an ingress PE router receives routes advertised from a directly connected CE router, it checks the received route against the VRF export policy for that VPN.

- If it matches, the route is converted to VPN-IPv4 format—that is, the route distinguisher is added to the route. The PE router then announces the route in VPN-IPv4 format to the remote PE routers. It also attaches a route target to each route learned from the directly connected sites. The route target attached to the route is based on the value of the VRF table's configured export target policy. The routes are then distributed using IBGP sessions, which are configured in the provider's core network.
- If the route from the CE router does not match, it is not exported to other PE routers, but it can still be used locally for routing, for example, if two CE routers in the same VPN are directly connected to the same PE router.

When an egress PE router receives a route, it checks it against the import policy on the IBGP session between the PE routers. If it is accepted, the router places the route into its `bgp.l3vpn.0` table. At the same time, the router checks the route against the VRF import policy for the VPN. If it matches, the route distinguisher is removed from the route and the route is placed into the VRF table (the *routing-instance-name.inet.0* table) in IPv4 format.

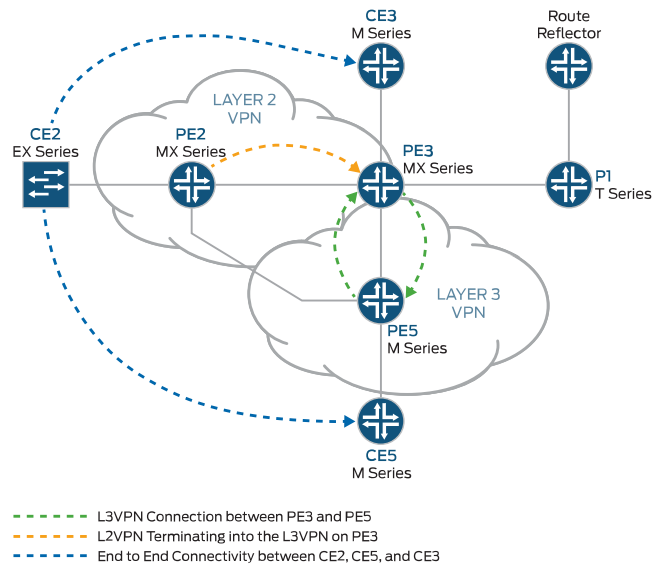
Figure 75 on page 817 shows the physical topology of a Layer 2 VPN-to-Layer 3 VPN interconnection.

**Figure 83: Physical Topology of a Layer 2 VPN Terminating into a Layer 3 VPN**



The logical topology of a Layer 2 VPN-to-Layer 3 VPN interconnection is shown in Figure 74 on page 816.

**Figure 84: Logical Topology of a Layer 2 VPN Terminating into a Layer 3 VPN**



The following definitions describe the meaning of the device abbreviations used in [Figure 75 on page 817](#) and [Figure 74 on page 816](#).

- Customer edge (CE) device—A device at the customer premises that provides access to the service provider's VPN over a data link to one or more provider edge (PE) routers.

Typically the CE device is an IP router that establishes an adjacency with its directly connected PE routers. After the adjacency is established, the CE router advertises the site's local VPN routes to the PE router and learns remote VPN routes from the PE router.

- Provider edge (PE) device—A device, or set of devices, at the edge of the provider network that presents the provider's view of the customer site.

PE routers exchange routing information with CE routers. PE routers are aware of the VPNs that connect through them, and PE routers maintain VPN state. A PE router is only required to maintain VPN routes for those VPNs to which it is directly attached. After learning local VPN routes from CE routers, a PE router exchanges VPN routing information with other PE routers using IBGP. Finally, when using MPLS to forward VPN data traffic across the provider's backbone, the ingress PE router functions as the ingress label-switching router (LSR) and the egress PE router functions as the egress LSR.

- Provider (P) device—A device that operates inside the provider's core network and does not directly interface to any CE.

Although the P device is a key part of implementing VPNs for the service provider's customers and may provide routing for many provider-operated tunnels that belong to different VPNs, it is not itself VPN-aware and does not maintain VPN state. Its principal role is allowing the service provider to scale its VPN offerings, for example, by acting as an aggregation point for multiple PE routers.

P routers function as MPLS transit LSRs when forwarding VPN data traffic between PE routers. P routers are required only to maintain routes to the provider's PE routers; they are not required to maintain specific VPN routing information for each customer site.

## Configuration

To interconnect a Layer 2 VPN with a Layer 3 VPN, perform these tasks:

- [Configuring the Base Protocols and Interfaces on page 967](#)
- [Configuring the VPN Interfaces on page 971](#)

### Configuring the Base Protocols and Interfaces

#### Step-by-Step Procedure

1. On each PE and P router, configure OSPF with traffic engineering extensions on all interfaces. Disable OSPF on the fxp0.0 interface.  
  

```
[edit protocols]
ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
```

```
 interface fxp0.0 {
 disable;
 }
 }
}
```

2. On all the core routers, enable MPLS on all interfaces. Disable MPLS on the fxp0.0 interface.

```
[edit protocols]
mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
}
```

3. On all the core routers, create an internal BGP peer group and specify the route reflector address (192.0.2.7) as the neighbor. Also enable BGP to carry Layer 2 VPLS network layer reachability information (NLRI) messages for this peer group by including the **signaling** statement at the **[edit protocols bgp group group-name family l2vpn]** hierarchy level.

```
[edit protocols]
bgp {
 group RR {
 type internal;
 local-address 192.0.2.2;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
}
```

4. On Router PE3, create an internal BGP peer group and specify the route reflector IP address (192.0.2.7) as the neighbor. Enable BGP to carry Layer 2 VPLS NLRI messages for this peer group and enable the processing of VPN-IPv4 addresses by including the **unicast** statement at the **[edit protocols bgp group group-name family inet-vpn]** hierarchy level.

```
[edit protocols]
bgp {
 group RR {
 type internal;
 local-address 192.0.2.3;
 family inet-vpn {
 unicast;
 }
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
}
```

5. For the Layer 3 VPN domain on Router PE3 and Router PE5, enable RSVP on all interfaces. Disable RSVP on the fxp0.0 interface.

```
[edit protocols]
rsvp {
 interface all;
 interface fxp0.0 {
 disable;
 }
}
```

6. On Router PE3 and Router PE5, create label-switched paths (LSPs) to the route reflector and the other PE routers. The following example shows the configuration on Router PE5.

```
[edit protocols]
mpls {
 label-switched-path to-RR {
 to 192.0.2.7;
 }
 label-switched-path to-PE2 {
 to 192.0.2.2;
 }
 label-switched-path to-PE3 {
 to 192.0.2.3;
 }
 label-switched-path to-PE4 {
 to 192.0.2.4;
 }
 label-switched-path to-PE1 {
 to 192.0.2.1;
 }
}
```

7. On Routers PE1, PE2, PE3, and PE5, configure the core interfaces with an IPv4 address and enable the MPLS address family. The following example shows the configuration of the xe-0/1/0 interface on Router PE2.

```
[edit]
interfaces {
 xe-0/1/0 {
 unit 0 {
 family inet {
 address 10.10.2.2/30;
 }
 family mpls;
 }
 }
}
```

8. On Router PE2 and Router PE3, configure LDP for the Layer 2 VPN MPLS signaling protocol for all interfaces. Disable LDP on the fxp0.0 interface. (RSVP can also be used.)

```
[edit protocols]
ldp {
 interface all;
```

```
interface fxp0.0 {
 disable;
}
}
```

9. On the route reflector, create an internal BGP peer group and specify the PE routers IP addresses as the neighbors.

```
[edit]
protocols {
 bgp {
 group RR {
 type internal;
 local-address 192.0.2.7;
 family inet {
 unicast;
 }
 family inet-vpn {
 unicast;
 }
 family l2vpn {
 signaling;
 }
 cluster 192.0.2.7;
 neighbor 192.0.2.1;
 neighbor 192.0.2.2;
 neighbor 192.0.2.4;
 neighbor 192.0.2.5;
 neighbor 192.0.2.3;
 }
 }
}
```

10. On the route reflector, configure MPLS LSPs towards Routers PE3 and PE5 to resolve the BGP next hops from inet.3 routing table.

```
[edit]
protocols {
 mpls {
 label-switched-path to-pe3 {
 to 192.0.2.3;
 }
 label-switched-path to-pe5 {
 to 192.0.2.5;
 }
 interface all;
 }
}
```

## Configuring the VPN Interfaces

### Step-by-Step Procedure

Router PE2 is one end of the Layer 2 VPN. Router PE3 is performing the Layer 2 VPN stitching between the Layer 2 VPN and the Layer 3 VPN. Router PE3 uses the logical tunnel interface (lt interface) configured with different logical interface units applied under two different Layer 2 VPN instances. The packet is looped though the lt interface configured on Router PE3. The configuration of Router PE5 contains the PE-CE interface.

1. On Router PE2, configure the ge-1/0/2 interface encapsulation. Include the encapsulation statement and specify the **ethernet-ccc** option (**vlan-ccc** encapsulation is also supported) at the **[edit interfaces ge-1/0/2]** hierarchy level. The encapsulation should be the same in a whole Layer 2 VPN domain (Routers PE2 and PE3). Also, configure interface lo0.

```
[edit]
interfaces {
 ge-1/0/2 {
 encapsulation ethernet-ccc;
 unit 0;
 }
 lo0 {
 unit 0 {
 family inet {
 address 192.0.2.2/24;
 }
 }
 }
}
```

2. On Router PE2, configure the routing instance at the **[edit routing-instances]** hierarchy level. Also, configure the Layer 2 VPN protocol at the **[edit routing-instances routing-instances-name protocols]** hierarchy level. Configure the remote site ID as 3. Site ID 3 represents Router PE3 (Hub-PE). The Layer 2 VPN is using LDP as the signaling protocol. Be aware that in the following example, both the routing instance and the protocol are named **l2vpn**.

```
[edit]
routing-instances {
 l2vpn { # routing instance
 instance-type l2vpn;
 interface ge-1/0/2.0;
 route-distinguisher 65000:2;
 vrf-target target:65000:2;
 protocols {
 l2vpn { # protocol
 encapsulation-type ethernet;
 site CE2 {
 site-identifier 2;
 interface ge-1/0/2.0 {
 remote-site-id 3;
 }
 }
 }
 }
 }
}
```

```

 }
}

```

3. On Router PE5, configure the Gigabit Ethernet interface for the PE-CE link **ge-2/0/0** and configure the **lo0** interface.

```

[edit interfaces]
ge-2/0/0 {
 unit 0 {
 family inet {
 address 198.51.100.8/24;
 }
 }
}
lo0 {
 unit 0 {
 }
}

```

4. On Router PE5, configure the Layer 3 VPN routing instance (**L3VPN**) at the **[edit routing-instances]** hierarchy level. Also configure BGP at the **[edit routing-instances L3VPN protocols]** hierarchy level.

```

[edit]
routing-instances {
 L3VPN {
 instance-type vrf;
 interface ge-2/0/0.0;
 route-distinguisher 65000:5;
 vrf-target target:65000:2;
 vrf-table-label;
 protocols {
 bgp {
 group ce5 {
 neighbor 198.51.100.2 {
 peer-as 200;
 }
 }
 }
 }
 }
}

```

5. In an MX Series router, such as Router PE3, you must create the tunnel services interface to be used for tunnel services. To create the tunnel service interface, include the **bandwidth** statement and specify the amount of bandwidth to reserve for tunnel services in gigabits per second at the **[edit chassis fpc slot-number pic slot-number tunnel-services]** hierarchy level.

```

[edit]
chassis {
 dump-on-panic;
 fpc 1 {
 pic 1 {
 tunnel-services {
 bandwidth 1g;
 }
 }
 }
}

```



```

 }
 }
}

```

6. On Router PE3, configure the Gigabit Ethernet interface.

Include the **address** statement at the **[edit interfaces ge-1/0/1.0 family inet]** hierarchy level and specify **198.51.100.9/24** as the IP address.

```

[edit]
interfaces {
 ge-1/0/1 {
 unit 0 {
 family inet {
 address 198.51.100.9/24;
 }
 }
 }
}

```

7. On Router PE3, configure the **lt-1/1/10.0** logical tunnel interface at the **[edit interfaces lt-1/1/10 unit 0]** hierarchy level. Router PE3 is the router that is *stitching* the Layer 2 VPN to the Layer 3 VPN using the logical tunnel interface. The configuration of the peer unit interfaces is what makes the interconnection.

To configure the interface, include the **encapsulation** statement and specify the **ethernet-ccc** option. Include the **peer-unit** statement and specify the logical interface unit 1 as the peer tunnel interface. Include the **family** statement and specify the **ccc** option.

```

[edit]
interfaces {
 lt-1/1/10 {
 unit 0 {
 encapsulation ethernet-ccc;
 peer-unit 1;
 family ccc;
 }
 }
}

```

8. On Router PE3, configure the **lt-1/1/10.1** logical tunnel interface at the **[edit interfaces lt-1/1/10 unit 1]** hierarchy level.

To configure the interface, include the **encapsulation** statement and specify the **ethernet** option. Include the **peer-unit** statement and specify the logical interface unit 0 as the peer tunnel interface. Include the **family** statement and specify the **inet** option. Include the **address** statement at the **[edit interfaces lt-1/1/10 unit 0]** hierarchy level and specify **198.51.100.7/24** as the IPv4 address.

```

[edit]
interfaces {
 lt-1/1/10 {
 unit 1 {
 encapsulation ethernet;
 peer-unit 0;
 family inet {

```

```

 address 198.51.100.7/24;
 }
}
}

```

9. On Router PE3, add the **lt** interface unit 1 to the routing instance at the **[edit routing-instances L3VPN]** hierarchy level. Configure the instance type as **vrf** with **lt** peer-unit 1 as a PE-CE interface to terminate the Layer 2 VPN on Router PE2 into the Layer 3 VPN on Router PE3.

```

[edit]
routing-instances {
 L3VPN {
 instance-type vrf;
 interface ge-1/0/1.0;
 interface lt-1/1/10.1;
 route-distinguisher 65000:33;
 vrf-target target:65000:2;
 vrf-table-label;
 protocols {
 bgp {
 export direct;
 group ce3 {
 neighbor 98.51.100.10 {
 peer-as 100;
 }
 }
 }
 }
 }
}

```

10. On Router PE3, add the **lt** interface unit 0 to the routing instance at the **[edit routing-instances protocols l2vpn]** hierarchy level. Also configure the same vrf target for the Layer 2 VPN and Layer 3 VPN routing instances, so that the routes can be leaked between the instances. The example configuration in the previous step shows the vrf target for the **L3VPN** routing instance. The following example shows the vrf target for the **l2vpn** routing instance.

```

[edit]
routing-instances {
 l2vpn {
 instance-type l2vpn;
 interface lt-1/1/10.0;
 route-distinguisher 65000:3;
 vrf-target target:65000:2;
 protocols {
 l2vpn {
 encapsulation-type ethernet;
 site CE3 {
 site-identifier 3;
 interface lt-1/1/10.0 {
 remote-site-id 2;
 }
 }
 }
 }
 }
}

```

```

 }
 }
}

```

11. On Router PE3, configure the **policy-statement** statement to export the routes learned from the directly connected **lt** interface unit 1 to all the CE routers for connectivity, if needed.

```

[edit]
policy-options {
 policy-statement direct {
 term 1 {
 from protocol direct;
 then accept;
 }
 }
}

```

**Results** The following output shows the full configuration of Router PE2:

```

Router PE2 interfaces {
 xe-0/1/0 {
 unit 0 {
 family inet {
 address 10.10.2.2/30;
 }
 family mpls;
 }
 }
 xe-0/2/0 {
 unit 0 {
 family inet {
 address 10.10.5.1/30;
 }
 family mpls;
 }
 }
 xe-0/3/0 {
 unit 0 {
 family inet {
 address 10.10.4.1/30;
 }
 family mpls;
 }
 }
 ge-1/0/2 {
 encapsulation ethernet-ccc;
 unit 0;
 }
 fxp0 {
 apply-groups [re0 re1];
 }
 lo0 {
 unit 0 {
 family inet {

```

```
 address 192.0.2.2/24;
 }
}
}
routing-options {
 static {
 route 172.16.0.0/8 next-hop 172.19.59.1;
 }
 autonomous-system 65000;
}
protocols {
 mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 bgp {
 group RR {
 type internal;
 local-address 192.0.2.2;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 }
 ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}
routing-instances {
 l2vpn {
 instance-type l2vpn;
 interface ge-1/0/2.0;
 route-distinguisher 65000:2;
 vrf-target target:65000:2;
 protocols {
 l2vpn {
 encapsulation-type ethernet;
 site CE2 {
 site-identifier 2;
 interface ge-1/0/2.0 {
```

```

 remote-site-id 3;
 }
}
}
}
}
}

```

The following output shows the final configuration of Router PE5:

```

Router PE5 interfaces {
 ge-0/0/0 {
 unit 0 {
 family inet {
 address 10.10.4.2/30;
 }
 family mpls;
 }
 }
 xe-0/1/0 {
 unit 0 {
 family inet {
 address 10.10.6.2/30;
 }
 family mpls;
 }
 }
 ge-1/0/0 {
 unit 0 {
 family inet {
 address 10.10.9.1/30;
 }
 family mpls;
 }
 }
 xe-1/1/0 {
 unit 0 {
 family inet {
 address 10.10.3.2/30;
 }
 family mpls;
 }
 }
 ge-2/0/0 {
 unit 0 {
 family inet {
 address 198.51.100.8/24;
 }
 }
 }
 lo0 {
 unit 0 {
 family inet {
 address 192.0.2.5/24;
 }
 }
 }
}

```

```
 }
 }
 routing-options {
 static {
 route 172.16.0.0/8 next-hop 172.19.59.1;
 }
 autonomous-system 65000;
 }
 protocols {
 rsvp {
 interface all {
 link-protection;
 }
 interface fxp0.0 {
 disable;
 }
 }
 mpls {
 label-switched-path to-RR {
 to 192.0.2.7;
 }
 label-switched-path to-PE2 {
 to 192.0.2.2;
 }
 label-switched-path to-PE3 {
 to 192.0.2.3;
 }
 label-switched-path to-PE4 {
 to 192.0.2.4;
 }
 label-switched-path to-PE1 {
 to 192.0.2.1;
 }
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 bgp {
 group to-rr {
 type internal;
 local-address 192.0.2.5;
 family inet-vpn {
 unicast;
 }
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
```

```

 disable;
 }
}
ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
}
}
routing-instances {
 L3VPN {
 instance-type vrf;
 interface ge-2/0/0.0;
 route-distinguisher 65000:5;
 vrf-target target:65000:2;
 vrf-table-label;
 protocols {
 bgp {
 group ce5 {
 neighbor 198.51.100.2 {
 peer-as 200;
 }
 }
 }
 }
 }
}
}

```

The following output shows the final configuration of Router PE3:

```

Router PE3 chassis {
 dump-on-panic;
 fpc 1 {
 pic 1 {
 tunnel-services {
 bandwidth 1g;
 }
 }
 }
 network-services ip;
 }
 interfaces {
 ge-1/0/1 {
 unit 0 {
 family inet {
 address 198.51.100.9/24;
 }
 }
 }
 lt-1/1/10 {
 unit 0 {
 encapsulation ethernet-ccc;
 peer-unit 1;
 family ccc;
 }
 }
 }
 }
 }

```

```
}
unit 1 {
 encapsulation ethernet;
 peer-unit 0;
 family inet {
 address 198.51.100.7/24;
 }
}
xe-2/0/0 {
 unit 0 {
 family inet {
 address 10.10.20.2/30;
 }
 family mpls;
 }
}
xe-2/1/0 {
 unit 0 {
 family inet {
 address 10.10.6.1/30;
 }
 family mpls;
 }
}
xe-2/2/0 {
 unit 0 {
 family inet {
 address 10.10.5.2/30;
 }
 family mpls;
 }
}
xe-2/3/0 {
 unit 0 {
 family inet {
 address 10.10.1.2/30;
 }
 family mpls;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.3/24;
 }
 }
}
}
routing-options {
 static {
 route 172.16.0.0/8 next-hop 172.19.59.1;
 }
 autonomous-system 65000;
}
protocols {
```



```

 rsvp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 mpls {
 label-switched-path to-RR {
 to 192.0.2.7;
 }
 label-switched-path to-PE2 {
 to 192.0.2.2;
 }
 label-switched-path to-PE5 {
 to 192.0.2.5;
 }
 label-switched-path to-PE4 {
 to 192.0.2.4;
 }
 label-switched-path to-PE1 {
 to 192.0.2.1;
 }
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 bgp {
 group RR {
 type internal;
 local-address 192.0.2.3;
 family inet-vpn {
 unicast;
 }
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 }
 ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}

```

```
policy-options {
 policy-statement direct {
 term 1 {
 from protocol direct;
 then accept;
 }
 }
}
routing-instances {
 L3VPN {
 instance-type vrf;
 interface ge-1/0/1.0;
 interface lt-1/1/10.1;
 route-distinguisher 65000:33;
 vrf-target target:65000:2;
 vrf-table-label;
 protocols {
 bgp {
 export direct;
 group ce3 {
 neighbor 98.51.100.10 {
 peer-as 100;
 }
 }
 }
 }
 }
 l2vpn {
 instance-type l2vpn;
 interface lt-1/1/10.0;
 route-distinguisher 65000:3;
 vrf-target target:65000:2;
 protocols {
 l2vpn {
 encapsulation-type ethernet;
 site CE3 {
 site-identifier 3;
 interface lt-1/1/10.0 {
 remote-site-id 2;
 }
 }
 }
 }
 }
}
```

## Verification

Verify the Layer 2 VPN-to-Layer 3 VPN interconnection:

- [Verifying Router PE2 VPN Interface on page 983](#)
- [Verifying Router PE3 VPN Interface on page 984](#)
- [Verifying End-to-End connectivity from Router CE2 to Router CE5 and Router CE3 on page 986](#)

### Verifying Router PE2 VPN Interface

**Purpose** Check that the Layer 2 VPN is up and working at the Router PE2 interface and that all the routes are there.

- Action** 1. Use the **show l2vpn connections** command to verify that the connection site ID is 3 for Router PE3 and that the status is **Up**.

```
user@PE2> show l2vpn connections
Layer-2 VPN connections:
Legend for connection status (St)
EI -- encapsulation invalid NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down NP -- interface hardware not present
CM -- control-word mismatch -> -- only outbound connection is up
CN -- circuit not provisioned <- -- only inbound connection is up
OR -- out of range Up -- operational
OL -- no outgoing label Dn -- down
LD -- local site signaled down CF -- call admission control failure
RD -- remote site signaled down SC -- local and remote site ID collision
LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status IL -- no incoming label
MM -- MTU mismatch MI -- Mesh-Group ID not available
BK -- Backup connection ST -- Standby connection
PF -- Profile parse failure PB -- Profile busy
RS -- remote site standby
```

```
Legend for interface status
Up -- operational
Dn -- down
```

```
Instance: l2vpn
Local site: CE2 (2)
 connection-site Type St Time last up # Up trans
 3 rmt Up Jan 7 14:14:37 2010 1
 Remote PE: 192.0.2.3, Negotiated control-word: Yes (Null)
 Incoming label: 800000, Outgoing label: 800001
 Local interface: ge-1/0/2.0, Status: Up, Encapsulation: ETHERNET
```

2. Use the **show route table** command to verify that the Layer 2 VPN route is present and that there is a next hop of **10.10.5.2** through the **xe-0/2/0.0** interface. The following output verifies that the Layer 2 VPN routes are present in the **l2vpn.l2vpn.0** table. Similar output should be displayed for Router PE3.

```
user@PE2> show route table l2vpn.l2vpn.0
l2vpn.l2vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

65000:2:2:3/96
 *[L2VPN/170/-101] 02:40:35, metric2 1
 Indirect
65000:3:3:1/96
 *[BGP/170] 02:40:35, localpref 100, from 192.0.2.7
 AS path: I
 > to 10.10.5.2 via xe-0/2/0.0
```

3. Verify that Router PE2 has a Layer 2 VPN MPLS label pointing to the LDP label to Router PE3 in both directions (PUSH and POP).

```

user@PE2> show route table mpls.0
mpls.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0 *[MPLS/0] 1w3d 08:57:41, metric 1
 Receive
1 *[MPLS/0] 1w3d 08:57:41, metric 1
 Receive
2 *[MPLS/0] 1w3d 08:57:41, metric 1
 Receive
300560 *[LDP/9] 19:45:53, metric 1
 > to 10.10.2.1 via xe-0/1/0.0, Pop
300560(S=0) *[LDP/9] 19:45:53, metric 1
 > to 10.10.2.1 via xe-0/1/0.0, Pop
301008 *[LDP/9] 19:45:53, metric 1
 > to 10.10.4.2 via xe-0/3/0.0, Swap 299856
301536 *[LDP/9] 19:45:53, metric 1
 > to 10.10.4.2 via xe-0/3/0.0, Pop
301536(S=0) *[LDP/9] 19:45:53, metric 1
 > to 10.10.4.2 via xe-0/3/0.0, Pop
301712 *[LDP/9] 16:14:52, metric 1
 > to 10.10.5.2 via xe-0/2/0.0, Swap 315184
301728 *[LDP/9] 16:14:52, metric 1
 > to 10.10.5.2 via xe-0/2/0.0, Pop
301728(S=0) *[LDP/9] 16:14:52, metric 1
 > to 10.10.5.2 via xe-0/2/0.0, Pop
800000 *[L2VPN/7] 02:40:35
 > via ge-1/0/2.0, Pop Offset: 4
ge-1/0/2.0 *[L2VPN/7] 02:40:35, metric 21
 > to 10.10.5.2 via xe-0/2/0.0, Push 800001 Offset: -4

```

**Meaning** The `l2vpn` routing instance is up at interface `ge-1/0/2` and the Layer 2 VPN route is shown in table `l2vpn.l2vpn.0`. Table `mpls.0` shows the Layer 2 VPN routes used to forward the traffic using an LDP label.

### Verifying Router PE3 VPN Interface

**Purpose** Check that the Layer 2 VPN connection from Router PE2 and Router PE3 is **Up** and working.

**Action** 1. Verify that the BGP session with the route reflector for the family `l2vpn-signaling` and the family `inet-vpn` is established.

```

user@PE3> show bgp summary
Groups: 2 Peers: 2 Down peers: 0
Table Tot Paths Act Paths Suppressed History Damp State Pending
bgp.l2vpn.0 1 1 0 0 0 0
bgp.L3VPN.0 1 1 0 0 0 0
Peer AS InPkt OutPkt OutQ Flaps Last Up/Dwn State|#Active /Received/Accepted/Damped...
192.0.2.7 65000 2063 2084 0 1 15:35:16 Establ
 bgp.l2vpn.0: 1/1/1/0
 bgp.L3VPN.0: 1/1/1/0
 L3VPN.inet.0: 1/1/1/0
 l2vpn.l2vpn.0: 1/1/1/0

```

2. The following output shows the `L3VPN.inet.0` routing table, which has Routers CE1, CE3, and CE5 listed.

```

user@PE3> show route table L3VPN.inet.0
L3VPN.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

198.51.100.17/24 *[Direct/0] 02:45:16
 > via lt-1/1/10.1
198.51.100.7/24 *[Local/0] 14:45:42
 Local via lt-1/1/10.1
198.51.100.18/24 *[BGP/170] 02:47:51, localpref 100, from 192.0.2.7
 AS path: I
 > to 10.10.6.2 via xe-2/1/0.0, Push 16
198.51.100.19/24 *[Direct/0] 15:26:24
 > via ge-1/0/1.0
198.51.100.9/24 *[Local/0] 15:26:24
 Local via ge-1/0/1.0

```

3. The following output verifies the Layer 2 VPN route and the label associated with it.

```

user@PE3> show route table l2vpn.l2vpn.0 detail
l2vpn.l2vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
65000:2:2:3/96 (1 entry, 1 announced)
 *BGP Preference: 170/-101
 Route Distinguisher: 65000:2
 Next hop type: Indirect
 Next-hop reference count: 4
 Source: 192.0.2.7
 Protocol next hop: 192.0.2.2
 Indirect next hop: 2 no-forward
 State: <Secondary Active Int Ext>
 Local AS: 65000 Peer AS: 65000
 Age: 2:45:52 Metric2: 1
 Task: BGP_65000.192.0.2.7+60585
 Announcement bits (1): 0-l2vpn-l2vpn
 AS path: I (Originator) Cluster list: 192.0.2.7
 AS path: Originator ID: 192.0.2.2
 Communities: target:65000:2 Layer2-info: encaps:ETHERNET,
control flags:Control-Word, mtu: 0, site preference: 100 Accepted
 Label-base: 800000, range: 2, status-vector: 0x0
 Localpref: 100
 Router ID: 192.0.2.7
 Primary Routing Table bgp.l2vpn.0

```

4. The following output show the L2VPN MPLS.0 route in the mpls.0 route table.

```

user@PE3> show route table mpls.0
mpls.0: 21 destinations, 21 routes (21 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0 *[MPLS/0] 1w3d 09:05:41, metric 1
 Receive
1 *[MPLS/0] 1w3d 09:05:41, metric 1
 Receive
2 *[MPLS/0] 1w3d 09:05:41, metric 1
 Receive
16 *[VPN/0] 15:59:24
 to table L3VPN.inet.0, Pop
315184 *[LDP/9] 16:21:53, metric 1
 > to 10.10.20.1 via xe-2/0/0.0, Pop
315184(S=0) *[LDP/9] 16:21:53, metric 1
 > to 10.10.20.1 via xe-2/0/0.0, Pop
315200 *[LDP/9] 01:13:44, metric 1
 to 10.10.20.1 via xe-2/0/0.0, Swap 625297

```

```

315216 > to 10.10.6.2 via xe-2/1/0.0, Swap 299856
 *[LDP/9] 16:21:53, metric 1
315216(S=0) > to 10.10.6.2 via xe-2/1/0.0, Pop
 *[LDP/9] 16:21:53, metric 1
315232 > to 10.10.6.2 via xe-2/1/0.0, Pop
 *[LDP/9] 16:21:45, metric 1
315232(S=0) > to 10.10.1.1 via xe-2/3/0.0, Pop
 *[LDP/9] 16:21:45, metric 1
315248 > to 10.10.1.1 via xe-2/3/0.0, Pop
 *[LDP/9] 16:21:53, metric 1
315248(S=0) > to 10.10.5.1 via xe-2/2/0.0, Pop
 *[LDP/9] 16:21:53, metric 1
315312 > to 10.10.5.1 via xe-2/2/0.0, Pop
 *[LDP/9] 16:21:53, metric 1
315312(S=0) > to 10.10.6.2 via xe-2/1/0.0, label-switched-path to-pe5
 *[RSVP/7] 15:02:40, metric 1
315328 > to 10.10.6.2 via xe-2/1/0.0, label-switched-path to-pe5
 *[RSVP/7] 15:02:40, metric 1
315360 > to 10.10.20.1 via xe-2/0/0.0, label-switched-path to-RR
 *[RSVP/7] 15:02:40, metric 1
316272 > to 10.10.20.1 via xe-2/0/0.0, label-switched-path to-RR
 *[RSVP/7] 01:13:27, metric 1
Bypass->10.10.9.1 > to 10.10.6.2 via xe-2/1/0.0, label-switched-path
316272(S=0) *[RSVP/7] 01:13:27, metric 1
 > to 10.10.6.2 via xe-2/1/0.0, label-switched-path
Bypass->10.10.9.1
800001 *[L2VPN/7] 02:47:33
 > via lt-1/1/10.0, Pop Offset: 4
lt-1/1/10.0 *[L2VPN/7] 02:47:33, metric2 1
 > to 10.10.5.1 via xe-2/2/0.0, Push 800000 Offset: -4

```

5. Use the **show route table mpls.0** command with the **detail** option to see the BGP attributes of the route such as next-hop type and label operations.

```

user@PE5> show route table mpls.0 detail
lt-1/1/10.0 (1 entry, 1 announced)
 *L2VPN Preference: 7
 Next hop type: Indirect
 Next-hop reference count: 2
 Next hop type: Router, Next hop index: 607
 Next hop: 10.10.5.1 via xe-2/2/0.0, selected
 Label operation: Push 800000 Offset: -4
 Protocol next hop: 192.0.2.2
 Push 800000 Offset: -4
 Indirect next hop: 8cae0a0 1048574
 State: <Active Int>
 Age: 2:46:34 Metric2: 1
 Task: Common L2 VC
 Announcement bits (2): 0-KRT 2-Common L2 VC
 AS path: I
 Communities: target:65000:2 Layer2-info: encaps:ETHERNET,
control flags:Control-Word, mtu: 0, site preference: 100

```

### Verifying End-to-End connectivity from Router CE2 to Router CE5 and Router CE3

**Purpose** Check the connectivity between Routers CE2, CE3, and CE5.

**Action** 1. Ping the Router CE3 IP address from Router CE2.

```
user@CE2> ping 98.51.100.10 # CE3 IP address
PING 98.51.100.10 (98.51.100.10): 56 data bytes
64 bytes from 98.51.100.10: icmp_seq=0 ttl=63 time=0.708 ms
64 bytes from 98.51.100.10: icmp_seq=1 ttl=63 time=0.610 ms
```

2. Ping the Router CE5 IP address from Router CE2.

```
user@CE2> ping 198.51.100.2 # CE5 IP address
PING 198.51.100.2 (198.51.100.2): 56 data bytes
64 bytes from 198.51.100.2: icmp_seq=0 ttl=62 time=0.995 ms
64 bytes from 198.51.100.2: icmp_seq=1 ttl=62 time=1.005 ms
```

**Related  
Documentation**

- [Understanding Layer 2 VPNs on page 121](#)
- [Understanding Layer 3 VPNs](#)
- [Interconnecting Layer 2 VPNs with Layer 3 VPNs Overview on page 963](#)





## Connecting Layer 2 Circuits to Other VPNs

- [Using the Layer 2 Interworking Interface to Interconnect a Layer 2 Circuit to a Layer 2 VPN on page 989](#)
- [Applications for Interconnecting a Layer 2 Circuit with a Layer 2 Circuit on page 990](#)
- [Example: Interconnecting a Layer 2 Circuit with a Layer 2 VPN on page 991](#)
- [Example: Interconnecting a Layer 2 Circuit with a Layer 2 Circuit on page 999](#)
- [Applications for Interconnecting a Layer 2 Circuit with a Layer 3 VPN on page 1015](#)
- [Example: Interconnecting a Layer 2 Circuit with a Layer 3 VPN on page 1015](#)

### Using the Layer 2 Interworking Interface to Interconnect a Layer 2 Circuit to a Layer 2 VPN

---

Instead of using a physical Tunnel PIC for looping the packet received from the Layer 2 circuit, the Layer 2 interworking interface uses Junos OS to stitch together both Layer 2 VPN routes.

To configure the interworking interface, include the **iw0** statement. The **iw0** statement is configured at the **[edit interfaces]** hierarchy level. This specifies the peering between two logical interfaces. This configuration is similar to the configuration for a logical tunnel interface. The logical Interfaces must be associated with the endpoints of a Layer 2 circuit and Layer 2 VPN connections.

```
[edit interfaces]
iw0 {
 unit 0 {
 peer-unit 1;
 }
 unit 1 {
 peer-unit 0;
 }
}
```

Configure the Layer 2 circuit protocol by including the **l2circuit** statement at the **[edit protocols]** hierarchy level and specifying the **neighbor** and **iw0** interface.

```
[edit protocols]
l2circuit {
 neighbor 192.0.2.0 {
 interface iw0.0;
 }
}
```

```
}
```

Configure the Layer 2 VPN connection, by including the ***routing-instance-name*** statement at the **[edit routing-instances]** hierarchy level and specifying the **instance-type l2vpn** option.

```
[edit routing-instances]
routing-instance-name {
 instance-type l2vpn;
 interface iw0.1;
 ...
 protocols {
 l2vpn {
 <l2vpn configuration>;
 }
 }
}
```

In addition to the **iw0** interface configuration, Layer 2 interworking **l2iw** protocols must be enabled. Without the **l2iw** configuration, the **l2iw** routes will not be formed, regardless of whether any **iw** interfaces are present. Within the **l2iw** protocols, only trace options can be configured in the standard fashion. The minimum configuration necessary for the feature to work is shown below:

```
[edit]
protocols {
 l2iw;
}
```

**Related  
Documentation**

- *Layer 2 Circuit Overview*
- [Example: Interconnecting a Layer 2 Circuit with a Layer 2 VPN on page 991](#)

---

## Applications for Interconnecting a Layer 2 Circuit with a Layer 2 Circuit

MPLS-based Layer 2 services are growing in demand among enterprise and service providers. This creates new challenges for service providers who want to provide end-to-end value-added services. There are various reasons to stitch different Layer 2 services to one another and to Layer 3 services, for example, to expand the service offerings and to expand geographically. Junos OS has various features to address the needs of the service provider.

In Layer 2 circuits with structure-aware TDM Circuit Emulation Service over Packet-Switched Network (CESoPSN) encapsulation, you can configure the payload size for virtual circuits that terminate on Layer 2 interworking (**iw**) logical interfaces. The payload size must be specified to enable stitching of LDP-signaled TDM pseudowires in environments where an interconnection between two Layer 2 circuits is required. You can include the **payload-size bytes** statement at the **[edit interfaces interface-name cesopsn-options]** hierarchy level, to define the size in bytes (from 32 through 1024 bytes).

Interconnecting a Layer 2 circuit with a Layer 2 circuit includes the following benefits:

- Interconnecting a Layer 2 circuit with a Layer 2 circuit enables the sharing of a service provider's core network infrastructure between Layer 2 circuit services, reducing the

cost of providing those services. A Layer 2 MPLS circuit enables service providers to create a Layer 2 circuit service over an existing IP and MPLS backbone.

- Service providers do not have to invest in separate Layer 2 equipment to provide Layer 2 circuit service. A service provider can configure a provider edge router to run any Layer 2 protocol. Customers who prefer to maintain control over most of the administration of their own networks want Layer 2 circuit connections with their service provider instead of a Layer 3 VPN connection.

**Related  
Documentation**

- [Example: Interconnecting a Layer 2 Circuit with a Layer 2 Circuit on page 999](#)

---

## Example: Interconnecting a Layer 2 Circuit with a Layer 2 VPN

This example provides a step-by-step procedure and commands for configuring and verifying a Layer 2 circuit to a Layer 2 VPN. It contains the following sections:

- [Requirements on page 991](#)
- [Overview and Topology on page 991](#)
- [Configuration on page 993](#)

### Requirements

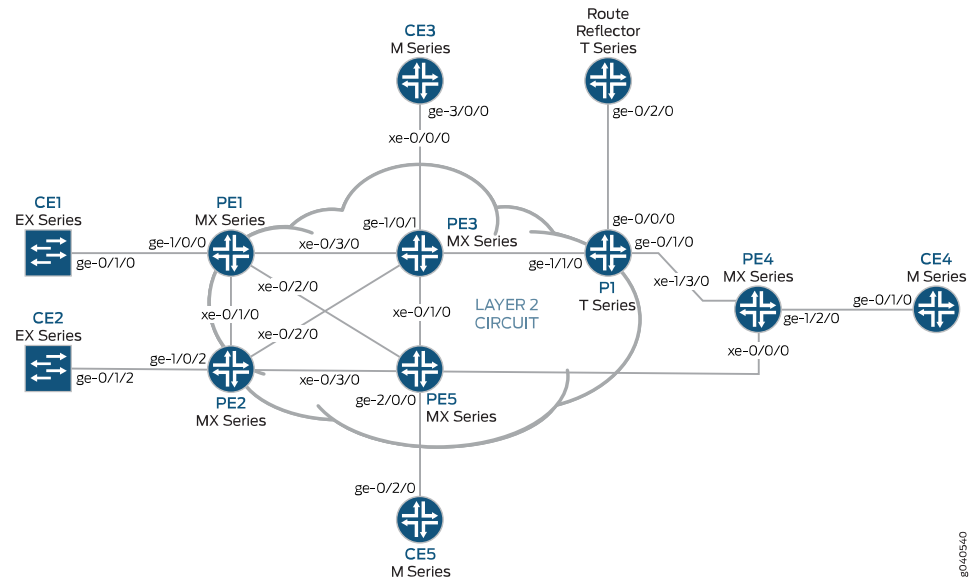
This example uses the following hardware and software components:

- Junos OS Release 9.3 or later
- 2 MX Series 3D Universal Edge Routers
- 2 M Series Multiservice Edge Router
- 1 T Series Core Router
- 1 EX Series Ethernet Switch

### Overview and Topology

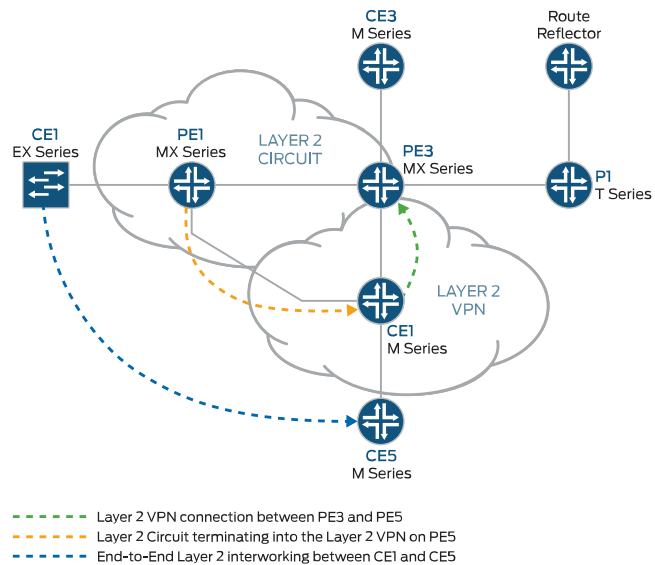
The physical topology of a Layer 2 circuit to a Layer 2 VPN connection is shown in [Figure 85 on page 992](#).

**Figure 85: Physical Topology of a Layer 2 Circuit to a Layer 2 VPN Connection**



The logical topology of a Layer 2 circuit to a Layer 2 VPN connection is shown in [Figure 86 on page 992](#).

**Figure 86: Logical Topology of a Layer 2 Circuit to a Layer 2 VPN Connection**



## Configuration



**NOTE:** In any configuration session, it is good practice to verify periodically 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
- **CE3** identifies the customer edge 3 (CE3) router
- **PE3** identifies the provider edge 3 (PE3) router
- **CE5** identifies the customer edge 5 (CE5) router
- **PE5** identifies the provider edge 5 (PE5) router

This example is organized in the following sections:

- [Configuring Protocols on the PE and P Routers on page 993](#)
- [Verification on page 997](#)

### Configuring Protocols on the PE and P Routers

#### Step-by-Step Procedure

In this example, all of the PE routers and P routers are configured with OSPF as the IGP protocol. The MPLS, LDP, and BGP protocols are enabled on all of the interfaces except **fxp0.0**. Core-facing interfaces are enabled with the MPLS address and inet address.

1. Configure all the PE and P routers with OSPF as the IGP. Enable the MPLS, LDP, and BGP protocols on all interfaces except **fxp0.0**. LDP is used as the signaling protocol on Router PE1 for the Layer 2 circuit. The following configuration snippet shows the protocol configuration for Router PE1:

```
[edit]
protocols {
 mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 bgp {
 group RR {
 type internal;
 local-address 192.0.2.1;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
 }
}
```

```

}
ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}
ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
}
}

```

2. Configure the PE and P routers with OSPF as the IGP. Enable the MPLS, LDP, and BGP protocols on all interfaces except **fxp0.0**. BGP is used as the signaling protocol on Router PE3 for the Layer 2 VPN. The following configuration snippet shows the protocol configuration for Router PE3:

```

[edit]
protocols {
 mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 bgp {
 group RR {
 type internal;
 local-address 192.0.2.3;
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 }
 ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}

```

```
}

```

### Step-by-Step Procedure

#### Configuring Interfaces

1. On Router PE1, configure the **ge-1/0/0** interface encapsulation. To configure the interface encapsulation, include the **encapsulation** statement and specify the **ethernet-ccc** option (vlan-ccc encapsulation is also supported). Configure the **ge-1/0/0.0** logical interface family for circuit cross-connect functionality. To configure the logical interface family, include the **family** statement and specify the **ccc** option. The encapsulation should be configured the same way for all routers in the Layer 2 circuit domain.

```
[edit interfaces]
ge-1/0/0 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.1/24;
 }
 }
}
```

2. Router PE5 is the router that is *stitching* the Layer 2 circuit to the Layer 2 VPN using the interworking interface. The configuration of the peer unit interfaces is what makes the interconnection.

On Router PE5, configure the **iw0** interface with two logical interfaces. To configure the **iw0** interface, include the **interfaces** statement and specify **iw0** as the interface name. For the unit 0 logical interface, include the **peer-unit** statement and specify the logical interface **unit 1** as the peer interface. For the unit 1 logical interface, include the **peer-unit** statement and specify the logical interface **unit 0** as the peer interface.

```
[edit interfaces]
iw0 {
 unit 0 {
 encapsulation ethernet-ccc;
 peer-unit 1;
 }
 unit 1 {
 encapsulation ethernet-ccc;
 peer-unit 0;
 }
}
```

3. On Router PE5, configure the logical loopback interface. The loopback interface is used to establish the targeted LDP sessions to Routers PE1 and PE5.

```
[edit interfaces]
lo0 {
 unit 0 {
 family inet {
```

```

 address 192.0.2.5/24;
 }
}

```

### Step-by-Step Procedure

#### Configuring the Layer 2 circuit protocol

1. On Router PE1, configure the IP address of the remote PE router with the **neighbor** statement. The loopback address and router ID of the PE neighbor is commonly the neighbor's IP address. To allow a Layer 2 circuit to be established even though the maximum transmission unit (MTU) configured on the PE router does not match the MTU configured on the remote PE router, include the **ignore-mtu-mismatch** statement.

```

[edit]
protocols {
 l2circuit {
 neighbor 192.0.2.5 {
 interface ge-1/0/0.0 {
 virtual-circuit-id 100;
 no-control-word;
 ignore-mtu-mismatch;
 }
 }
 }
}

```

2. On Router PE5, configure the IP address of the remote PE router. To configure the IP address of the remote PE router, include the **neighbor** statement and specify the IP address of the loopback interface on Router PE1. Configure the virtual circuit ID to be the same as the virtual circuit ID on the neighbor router. To allow a Layer 2 circuit to be established even though the MTU configured on the local PE router does not match the MTU configured on the remote PE router, include the **ignore-mtu-mismatch** statement. Also disable the use of the control word for demultiplexing by including the **no-control-word** statement.

```

[edit protocols]
l2circuit {
 neighbor 192.0.2.1 {
 interface iw0.0 {
 virtual-circuit-id 100;
 no-control-word;
 ignore-mtu-mismatch;
 }
 }
}

```

3. On Router PE5, configure the Layer 2 VPN protocols by including the **l2vpn** statement at the **[edit routing-instances routing-instances-name protocols]** hierarchy level. To configure the **iw0** interface, include the **interfaces** statement and specify **iw0** as the interface name. The **iw0** interface is configured under the Layer 2 VPN protocols to receive the looped packet from the **iw0.1** logical interface. The **l2vpn** protocol is configured on Router PE5 with site CE5, which is configured in the BGP L2VPN



routing instance. Router CE1 has communication to Router CE5, through the Layer 2 interworking configuration on Router PE5.

```
[edit]
routing-instances {
 L2VPN {
 instance-type l2vpn;
 interface ge-2/0/0.0;
 interface iw0.1;
 route-distinguisher 65000:5;
 vrf-target target:65000:2;
 protocols {
 l2vpn {
 encapsulation-type ethernet;
 site CE5 {
 site-identifier 5;
 interface ge-2/0/0.0 {
 remote-site-id 3;
 }
 }
 site l2-circuit {
 site-identifier 6;
 interface iw0.1 {
 remote-site-id 3;
 }
 }
 }
 }
 }
}
```

4. In addition to the **iw0** interface configuration, the Layer 2 interworking **l2iw** protocol must be configured. Without the **l2iw** protocol configuration, the Layer 2 interworking routes are not formed, regardless of whether any **iw** interfaces are present.

On Router PE5, configure the **l2iw** protocol. To configure the protocol, include the **l2iw** statement at the **[edit protocols]** hierarchy level.

```
[edit]
protocols {
 l2iw;
}
```

### Verification

**Step-by-Step Procedure** Verifying the Layer 2 Circuit Connection on Router PE1.

1. On Router PE1, use the **show l2circuit connections** command to verify that the Layer 2 Circuit from Router PE1 to Router PE5 is **Up**.

```
user@PE1> show l2circuit connections
Layer-2 Circuit Connections:
Legend for connection status (St)
EI -- encapsulation invalid NP -- interface h/w not present
MM -- mtu mismatch Dn -- down
EM -- encapsulation mismatch VC-Dn -- Virtual circuit Down
CM -- control-word mismatch Up -- operational
```

VM -- vlan id mismatch                      CF -- Call admission control failure  
 OL -- no outgoing label                      IB -- TDM incompatible bitrate  
 NC -- intf encaps not CCC/TCC              TM -- TDM misconfiguration  
 BK -- Backup Connection                    ST -- Standby Connection  
 CB -- rcvd cell-bundle size bad          XX -- unknown  
 SP -- Static Pseudowire

#### Legend for interface status

Up -- operational

Dn -- down

Neighbor: 192.0.2.5

| Interface          | Type | St | Time last up        | # Up trans |
|--------------------|------|----|---------------------|------------|
| ge-1/0/0.0(vc 100) | rmt  | Up | Jan 3 22:00:49 2010 | 1          |

Remote PE: 192.0.2.5, Negotiated control-word: No  
 Incoming label: 301328, Outgoing label: 300192  
 Local interface: ge-1/0/0.0, Status: Up, Encapsulation: ETHERNET

- On Router PE5, use the **show l2vpn connections** command to verify that the Layer 2 VPN connection is **Up** using the **iw0** peer interface of the Layer 2 circuit.

user@PE5> show l2vpn connections

Instance: L2VPN

Local site: CE5 (5)

| connection-site | Type | St | Time last up        | # Up trans |
|-----------------|------|----|---------------------|------------|
| l2-circuit (6)  | loc  | OR |                     |            |
| 3               | rmt  | Up | Jan 3 22:51:12 2010 | 1          |

Remote PE: 192.0.2.3, Negotiated control-word: Yes (Null)  
 Incoming label: 800258, Outgoing label: 800000  
 Local interface: ge-2/0/0.0, Status: Up, Encapsulation: ETHERNET

Local site: l2-circuit (6)

| connection-site | Type | St | Time last up        | # Up trans |
|-----------------|------|----|---------------------|------------|
| CE5 (5)         | loc  | OR |                     |            |
| 3               | rmt  | Up | Jan 3 22:56:38 2010 | 1          |

Remote PE: 192.0.2.3, Negotiated control-word: Yes (Null)  
 Incoming label: 800262, Outgoing label: 800001  
 Local interface: iw0.1, Status: Up, Encapsulation: ETHERNET

#### Step-by-Step Procedure

Verifying that the Layer 2 Circuit is terminating into the Layer 2 VPN connection.

- On Router PE5, use the **show l2circuit connections** command to verify that the Layer 2 circuit is **Up** using the **iw0** interface. This will be looped through the **iwo.1** interface to the Layer 2 VPN.

user@PE5> show l2circuit connections

Layer-2 Circuit Connections:

Neighbor: 192.0.2.1

| Interface     | Type | St | Time last up        | # Up trans |
|---------------|------|----|---------------------|------------|
| iw0.0(vc 100) | rmt  | Up | Jan 3 21:59:07 2010 | 1          |

Remote PE: 192.0.2.1, Negotiated control-word: No  
 Incoming label: 300192, Outgoing label: 301328

- On Router PE 5, use the **show route table mpls.0** command to verify the Layer 2 circuit and Layer 2 VPN routes. In the example below, the Layer 2 circuit is associated with LDP label **301328** and the Layer 2 VPN is associated with LDP label **800001**. Notice the two **iw0** interfaces that are used for the Layer 2 interworking route.

user@PE5> show route table mpls.0

```

mpls.0: 18 destinations, 20 routes (18 active, 2 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0 *[MPLS/0] 5d 20:07:31, metric 1
 Receive
1 *[MPLS/0] 5d 20:07:31, metric 1
 Receive
2 *[MPLS/0] 5d 20:07:31, metric 1
 Receive
299776 *[LDP/9] 2d 03:00:51, metric 1
300048 *[LDP/9] 2d 03:00:49, metric 1
 > to 10.10.6.1 via xe-0/1/0.0, Pop
300048(S=0) *[LDP/9] 2d 03:00:49, metric 1
 > to 10.10.6.1 via xe-0/1/0.0, Pop
300192 *[L2IW/6] 19:11:05, metric2 1
 > to 10.10.6.1 via xe-0/1/0.0, Swap 800001
 [L2CKT/7] 20:08:36
 > via iw0.0, Pop
800258 *[L2VPN/7] 19:16:31
 > via ge-2/0/0.0, Pop Offset: 4
800262 *[L2IW/6] 19:11:05, metric2 1 > to 10.10.3.1 via xe-1/1/0.0, Swap 301328 [L2VPN/7]
19:11:05 > via iw0.1, Pop Offset: 4ge-2/0/0.0 *[L2VPN/7] 19:16:31, metric2 1
 > to 10.10.6.1 via xe-0/1/0.0, Push 800000 Offset: -4
iw0.0 *[L2CKT/7] 20:08:36, metric2 1
 > to 10.10.3.1 via xe-1/1/0.0, Push 301328
iw0.1 *[L2VPN/7] 19:11:05, metric2 1
 > to 10.10.6.1 via xe-0/1/0.0, Push 800001 Offset: -4

```

**Related Documentation** • [Applications for Interconnecting a Layer 2 Circuit with a Layer 2 Circuit on page 990](#)

## Example: Interconnecting a Layer 2 Circuit with a Layer 2 Circuit

This example provides a step-by-step procedure and commands for configuring and verifying a Layer 2 circuit to a Layer 2 circuit interconnection. It contains the following sections:

- [Requirements on page 999](#)
- [Overview and Topology on page 1000](#)
- [Configuration on page 1001](#)

### Requirements

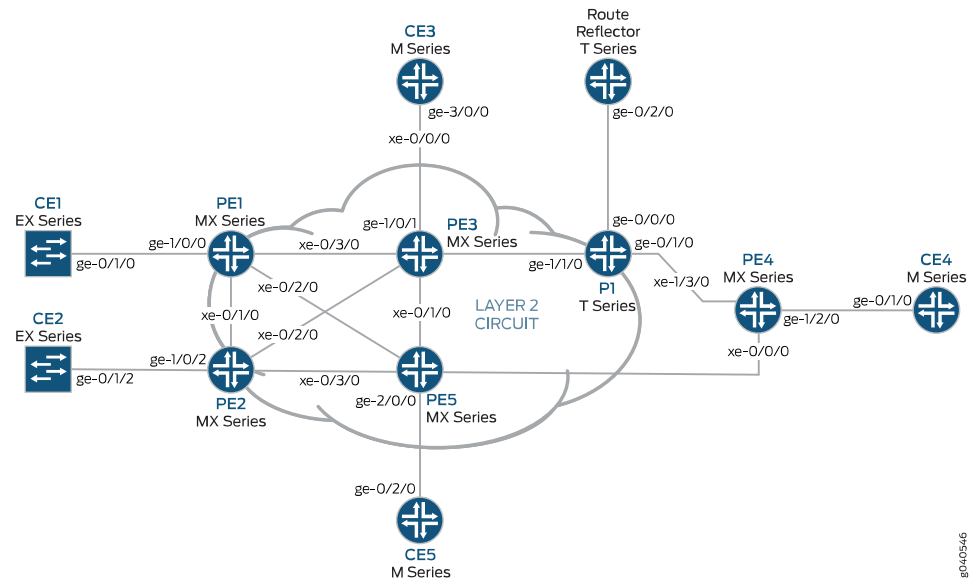
This example uses the following hardware and software components:

- Junos OS Release 9.3 or later
- 2 MX Series routers
- 2 M Series routers
- 1 T Series router
- 1 EX Series router

## Overview and Topology

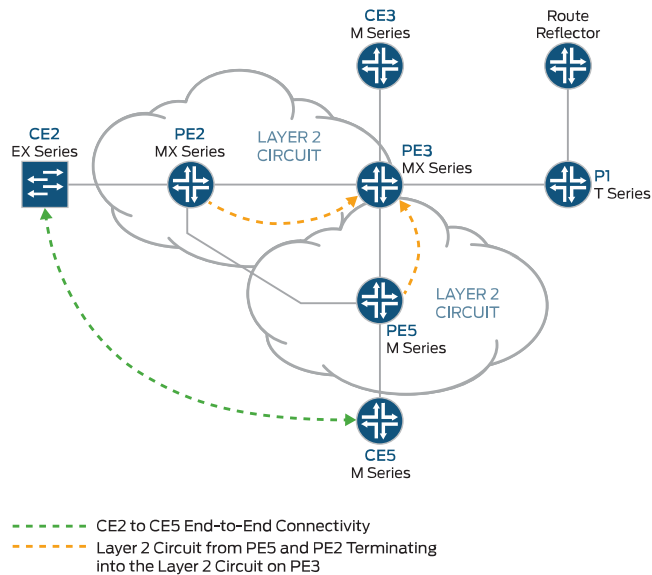
The physical topology of a Layer 2 circuit to Layer 2 circuit interconnection is shown in [Figure 87 on page 1000](#)

**Figure 87: Physical Topology of a Layer 2 Circuit Terminating into a Layer 2 Circuit**



The logical topology of a Layer 2 circuit to Layer 2 circuit interconnection is shown in [Figure 88 on page 1000](#)

**Figure 88: Logical Topology of a Layer 2 Circuit Terminating into a Layer 2 Circuit**



## Configuration



**NOTE:** In any configuration session, it is good practice to verify periodically 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:

- **CE2** identifies the customer edge 2 (CE2) router
- **PE1** identifies the provider edge 1 (PE1) router
- **CE3** identifies the customer edge 3 (CE3) router
- **PE3** identifies the provider edge 3 (PE3) router
- **CE5** identifies the customer edge 5 (CE5) router
- **PE5** identifies the provider edge 5 (PE5) router

This example contains the following procedures:

- [Configuring PE Router Customer-facing and Loopback Interfaces on page 1001](#)
- [Configuring Core-facing Interfaces on page 1002](#)
- [Configuring Protocols on page 1004](#)
- [Configuring the Layer 2 Circuits on page 1005](#)
- [Interconnecting the Layer 2 Circuits on page 1007](#)
- [Verifying the Layer 2 Circuit to Layer 2 Circuit Interconnection on page 1008](#)
- [Results on page 1011](#)

### Configuring PE Router Customer-facing and Loopback Interfaces

#### Step-by-Step Procedure

To begin building the interconnection, configure the interfaces on the PE routers. If your network contains provider (P) routers, configure the interfaces on the P routers also. This example shows the configuration for Router PE1 and Router PE5.

1. On Router PE1, configure the **ge-1/0/0** interface encapsulation. To configure the interface encapsulation, include the **encapsulation** statement and specify the **ethernet-ccc** option (vlan-ccc encapsulation is also supported). Configure the **ge-1/0/0.0** logical interface family for circuit cross-connect functionality. To configure the logical interface family, include the **family** statement and specify the **ccc** option.

```
[edit interfaces]
ge-1/0/0 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
}
lo0 {
```

```

 unit 0 {
 family inet {
 address 192.0.2.1/24;
 }
 }
 }
}

```

2. On Router PE5, configure the **ge-2/0/0** interface encapsulation. To configure the interface encapsulation, include the **encapsulation** statement and specify the **ethernet-ccc** option. Configure the **ge-2/0/0.0** logical interface family for circuit cross-connect functionality. To configure the logical interface family, include the **family** statement and specify the **ccc** option

```

[edit interfaces]
ge-2/0/0 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.5/24;
 }
 }
}
}

```

3. On Router PE3, configure the logical loopback interface. The loopback interface is used to establish the targeted LDP sessions to Routers PE1 and PE5.

```

[edit interfaces]
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.3/24;
 }
 }
}
}

```

### Configuring Core-facing Interfaces

#### Step-by-Step Procedure

This procedure describes how to configure the core-facing interfaces on the PE routers. This example does not include all the core-facing interfaces shown in the physical topology illustration. Enable the **mpls** and **inet** address families on the core-facing interfaces.

1. On Router PE1, configure the **xe-0/3/0** interface. Include the **family** statement and specify the **inet** address family. Include the **address** statement and specify **10.10.1.1/30** as the interface address. Include the **family** statement and specify the **mpls** address family.

```

[edit interfaces]
xe-0/3/0 {
 unit 0 {

```

```

 family inet {
 address 10.10.1.1/30;
 }
 family mpls;
 }
}

```

2. On Router PE3, configure the core-facing interfaces. Include the **family** statement and specify the **inet** address family. Include the **address** statement and specify the IPv4 addresses shown in the example as the interface addresses. Include the **family** statement and specify the **mpls** address family. In the example, the **xe-0/0/0** interface is connected to the route reflector, the **xe-0/1/0** interface is connected to Router PE5, the **xe-0/2/0** interface is connected to Router PE2, and the **xe-0/3/0** interface is connected to Router PE1.

```

[edit interfaces]
xe-0/0/0 {
 unit 0 {
 family inet {
 address 10.10.20.2/30;
 }
 family mpls;
 }
}
xe-0/1/0 {
 unit 0 {
 family inet {
 address 10.10.6.1/30;
 }
 family mpls;
 }
}
xe-0/2/0 {
 unit 0 {
 family inet {
 address 10.10.5.2/30;
 }
 family mpls;
 }
}
xe-0/3/0 {
 unit 0 {
 family inet {
 address 10.10.1.2/30;
 }
 family mpls;
 }
}

```

3. On Router PE5, configure the **xe-0/1/0** interface. Include the **family** statement and specify the **inet** address family. Include the **address** statement and specify **10.10.6.2/30** as the interface address. Include the **family** statement and specify the **mpls** address family.

```

[edit interfaces]
xe-0/1/0 {

```

```
unit 0 {
 family inet {
 address 10.10.6.2/30;
 }
 family mpls;
}
}
```

---

### Configuring Protocols

#### Step-by-Step Procedure

This procedure describes how to configure the protocols used in this example. If your network contains P routers, configure the protocols on the P routers also.

Configure all of the PE routers and P routers with OSPF as the IGP protocol. Enable MPLS and LDP protocols on all of the interfaces except **fxp0.0**.

1. On Router PE1, enable OSPF as the IGP. Enable the MPLS and LDP protocols on all interfaces except **fxp0.0**. LDP is used as the signaling protocol on Router PE1 for the Layer 2 circuit. The following configuration snippet shows the protocol configuration for Router PE1:

```
[edit]
protocols {
 mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 }
 ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}
```

2. Configure the PE and P routers with OSPF as the IGP. Enable the MPLS and LDP protocols on all interfaces except **fxp0.0**. The following configuration snippet shows the protocol configuration for Router PE3:

```
[edit]
protocols {
 mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}
```



```

 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 }
 ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}

```

### Configuring the Layer 2 Circuits

#### Step-by-Step Procedure

This procedure describes how to configure the Layer 2 circuits.



**NOTE:** In this example the **ignore-mtu-mismatch** statement is required for the circuit to come up.

1. On Router PE1, configure the Layer 2 circuit. Include the **l2circuit** statement. Include the **neighbor** statement and specify the loopback IPv4 address of Router PE3 as the neighbor. Include the interface statement and specify **ge-1/0/0.0** as the logical interface that is participating in the Layer 2 circuit. Include the **virtual-circuit-id** statement and specify **100** as the identifier. Include the **ignore-mtu-mismatch** statement to allow a Layer 2 circuit to be established even though the maximum transmission unit (MTU) configured on the local PE router does not match the MTU configured on the remote PE router.

```

[edit]
protocols {
 l2circuit {
 neighbor 192.0.2.3 {
 interface ge-1/0/0.0 {
 virtual-circuit-id 100;
 ignore-mtu-mismatch;
 }
 }
 }
}

```

2. On Router PE5, configure the Layer 2 circuit. Include the **l2circuit** statement. Include the **neighbor** statement and specify the loopback IPv4 address of Router PE3 as the neighbor. Include the interface statement and specify **ge-2/0/0.0** as the logical interface that is participating in the Layer 2 circuit. Include the **virtual-circuit-id**

statement and specify **200** as the identifier. Include the **ignore-mtu-mismatch** statement to allow a Layer 2 circuit to be established even though the MTU configured on the local PE router does not match the MTU configured on the remote PE router.

```
[edit]
protocols {
 l2circuit {
 neighbor 192.0.2.3 {
 interface ge-2/0/0.0 {
 virtual-circuit-id 200;
 ignore-mtu-mismatch;
 }
 }
 }
}
```

3. On Router PE3, configure the Layer 2 circuit to Router PE1. Include the **l2circuit** statement. Include the **neighbor** statement and specify the loopback IPv4 address of Router PE1 as the neighbor. Include the interface statement and specify **iw0.0** as the logical interworking interface that is participating in the Layer 2 circuit. Include the **virtual-circuit-id** statement and specify **100** as the identifier. Include the **ignore-mtu-mismatch** statement to allow a Layer 2 circuit to be established even though the MTU configured on the local PE router does not match the MTU configured on the remote PE router.

On Router PE3, configure the Layer 2 circuit to Router PE5. Include the **l2circuit** statement. Include the **neighbor** statement and specify the loopback IPv4 address of Router PE5 as the neighbor. Include the interface statement and specify **iw0.1** as the logical interworking interface that is participating in the Layer 2 circuit. Include the **virtual-circuit-id** statement and specify **200** as the identifier. Include the **ignore-mtu-mismatch** statement.

```
[edit protocols]
l2circuit {
 neighbor 192.0.2.1 {
 interface iw0.0 {
 virtual-circuit-id 100;
 ignore-mtu-mismatch;
 }
 }
 neighbor 192.0.2.5 {
 interface iw0.1 {
 virtual-circuit-id 200;
 ignore-mtu-mismatch;
 }
 }
}
```

### Interconnecting the Layer 2 Circuits

**Step-by-Step Procedure** Router PE3 is the router that is *stitching* the Layer 2 circuits together using the interworking interface. The configuration of the peer unit interfaces is what makes the interconnection.

1. On Router PE3, configure the **iw0.0** interface. Include the **encapsulation** statement and specify the **ethernet-ccc** option. Include the **peer-unit** statement and specify the logical interface unit 1 as the peer tunnel interface.

On Router PE3, configure the **iw0.1** interface. Include the **encapsulation** statement and specify the **ethernet-ccc** option. Include the **peer-unit** statement and specify the logical interface unit 0 as the peer tunnel interface.

```
[edit interfaces]
iw0 {
 unit 0 {
 encapsulation ethernet-ccc;
 peer-unit 1;
 }
 unit 1 {
 encapsulation ethernet-ccc;
 peer-unit 0;
 }
}
```

2. On Router PE3, configure the Layer 2 interworking **l2iw** protocol. To configure the Layer 2 interworking protocol, include the **l2iw** statement at the **[edit protocols]** hierarchy level.

```
[edit]
protocols {
 l2iw;
}
```

3. On each router, commit the configuration.

```
user@host> commit check
configuration check succeeds
user@host> commit
```

## Verifying the Layer 2 Circuit to Layer 2 Circuit Interconnection

**Step-by-Step Procedure** Verify that the Layer 2 circuit connection on Router PE1 is up, the LDP neighbors are correct, and the MPLS label operations are correct.

1. On Router PE1, use the **show l2circuit connections** command to verify that the Layer 2 circuit from Router PE1 to Router PE3 is Up.

```
user@PE1> show l2circuit connections
Layer-2 Circuit Connections:
Legend for connection status (St)
EI -- encapsulation invalid NP -- interface h/w not present
MM -- mtu mismatch Dn -- down
EM -- encapsulation mismatch VC-Dn -- Virtual circuit Down
CM -- control-word mismatch Up -- operational
VM -- vlan id mismatch CF -- Call admission control failure
OL -- no outgoing label IB -- TDM incompatible bitrate
NC -- intf encaps not CCC/TCC TM -- TDM misconfiguration
BK -- Backup Connection ST -- Standby Connection
CB -- rcvd cell-bundle size bad XX -- unknown
SP -- Static Pseudowire
```

Legend for interface status

Up -- operational

Dn -- down

Neighbor: 192.0.2.3

```
Interface Type St Time last up # Up trans
ge-1/0/0.0(vc 100) rmt Up Jan 5 22:00:49 2010 1
Remote PE: 192.0.2.3, Negotiated control-word: Yes (Null)
Incoming label: 301328, Outgoing label: 314736
Local interface: ge-1/0/0.0, Status: Up, Encapsulation: ETHERNET
```

2. On Router PE1, use the **show ldp neighbor** command to verify that the IPv4 address of Router PE3 is shown as the LDP neighbor.

```
user@PE1> show ldp neighbor
```

| Address   | Interface | Label space ID | Hold time |
|-----------|-----------|----------------|-----------|
| 192.0.2.3 | lo0.0     | 192.0.2.3:0    | 41        |

3. On Router PE1, use the **show route table mpls.0** command to verify the Layer 2 circuit is using the LDP label to Router PE3 in both directions (Push and Pop). In the example below, the Layer 2 circuit is associated with LDP label **301328**.

```
user@PE1> show route table mpls.0
```

```
mpls.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
```

|             |                                                                      |
|-------------|----------------------------------------------------------------------|
| 0           | *[MPLS/0] 1w1d 08:25:39, metric 1<br>Receive                         |
| 1           | *[MPLS/0] 1w1d 08:25:39, metric 1<br>Receive                         |
| 2           | *[MPLS/0] 1w1d 08:25:39, metric 1<br>Receive                         |
| 300432      | *[LDP/9] 3d 01:13:57, metric 1<br>> to 10.10.2.2 via xe-0/1/0.0, Pop |
| 300432(S=0) | *[LDP/9] 3d 01:13:57, metric 1<br>> to 10.10.2.2 via xe-0/1/0.0, Pop |
| 300768      | *[LDP/9] 3d 01:13:57, metric 1                                       |

```

> to 10.10.3.2 via xe-0/2/0.0, Pop
300768(S=0) * [LDP/9] 3d 01:13:57, metric 1
> to 10.10.3.2 via xe-0/2/0.0, Pop
300912 * [LDP/9] 3d 01:13:57, metric 1
> to 10.10.3.2 via xe-0/2/0.0, Swap 299856
301264 * [LDP/9] 3d 01:13:53, metric 1
> to 10.10.1.2 via xe-0/3/0.0, Swap 308224
301312 * [LDP/9] 3d 01:13:56, metric 1
> to 10.10.1.2 via xe-0/3/0.0, Pop
301312(S=0) * [LDP/9] 3d 01:13:56, metric 1
> to 10.10.1.2 via xe-0/3/0.0, Pop
301328 * [L2CKT/7] 02:33:26 > via ge-1/0/0.0, Pop Offset: 4
ge-1/0/0.0 * [L2CKT/7] 02:33:26, metric 2 1 > to 10.10.1.2 via xe-0/3/0.0,
Push 314736 Offset: -4

```

4. On Router PE3, use the **show l2circuit connections** command to verify that the Layer 2 circuit from Router PE3 to Router PE5 is **Up**, that the Layer 2 circuit from Router PE3 to Router PE1 is **Up**, that the connections to Router PE1 and Router PE5 use the **iw0** interface, and that the status for both local **iw0** interfaces is **Up**.

```
user@PE3> show l2circuit connections
```

```
Layer-2 Circuit Connections:
```

```
Legend for connection status (St)
```

```

EI -- encapsulation invalid NP -- interface h/w not present
MM -- mtu mismatch Dn -- down
EM -- encapsulation mismatch VC-Dn -- Virtual circuit Down
CM -- control-word mismatch Up -- operational
VM -- vlan id mismatch CF -- Call admission control failure
OL -- no outgoing label IB -- TDM incompatible bitrate
NC -- intf encaps not CCC/TCC TM -- TDM misconfiguration
BK -- Backup Connection ST -- Standby Connection
CB -- rcvd cell-bundle size bad XX -- unknown
SP -- Static Pseudowire

```

```
Legend for interface status
```

```
Up -- operational
```

```
Dn -- down
```

```
Neighbor: 192.0.2.1
```

```

Interface Type St Time last up # Up trans
iw0.0(vc 100) rmt Up Jan 5 13:50:14 2010 1
Remote PE: 192.0.2.1, Negotiated control-word: Yes (Null)
Incoming label: 314736, Outgoing label: 301328
Local interface: iw0.0, Status: Up, Encapsulation: ETHERNET

```

```
Neighbor: 192.0.2.5
```

```

Interface Type St Time last up # Up trans
iw0.1(vc 200) rmt Up Jan 5 13:49:58 2010 1
Remote PE: 192.0.2.5, Negotiated control-word: Yes (Null)
Incoming label: 314752, Outgoing label: 300208
Local interface: iw0.1, Status: Up, Encapsulation: ETHERNET

```

5. On Router PE3, use the **show ldp neighbor** command to verify that the correct IPv4 addresses are shown as the LDP neighbor.

```
user@PE3> show ldp neighbor
```

| Address   | Interface | Label space ID | Hold time |
|-----------|-----------|----------------|-----------|
| 192.0.2.1 | lo0.0     | 192.0.2.1:0    | 44        |
| 192.0.2.2 | lo0.0     | 192.0.2.2:0    | 42        |
| 192.0.2.4 | lo0.0     | 192.0.2.4:0    | 31        |
| 192.0.2.5 | lo0.0     | 192.0.2.5:0    | 44        |

6. On Router PE3, use the **show route table mpls.0** command to verify that the **mpls.0** routing table is populated with the Layer 2 interworking routes. Notice that in this example, the router is swapping label **314736** received from Router PE1 on the **iw0.0** to label **301328**.

```

user@PE3> show route table mpls.0
mpls.0: 16 destinations, 18 routes (16 active, 2 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0 *[MPLS/0] 1w1d 08:28:24, metric 1
 Receive
1 *[MPLS/0] 1w1d 08:28:24, metric 1
 Receive
2 *[MPLS/0] 1w1d 08:28:24, metric 1
 Receive
308160 *[LDP/9] 3d 01:16:55, metric 1
 > to 10.10.1.1 via xe-0/3/0.0, Pop
308160(S=0) *[LDP/9] 3d 01:16:55, metric 1
 > to 10.10.1.1 via xe-0/3/0.0, Pop
308176 *[LDP/9] 3d 01:16:54, metric 1
 > to 10.10.6.2 via xe-0/1/0.0, Pop
308176(S=0) *[LDP/9] 3d 01:16:54, metric 1
 > to 10.10.6.2 via xe-0/1/0.0, Pop
308192 *[LDP/9] 00:21:40, metric 1
 > to 10.10.20.1 via xe-0/0/0.0, Swap 601649
 > to 10.10.6.2 via xe-0/1/0.0, Swap 299856
308208 *[LDP/9] 3d 01:16:54, metric 1
 > to 10.10.5.1 via xe-0/2/0.0, Pop
308208(S=0) *[LDP/9] 3d 01:16:54, metric 1
 > to 10.10.5.1 via xe-0/2/0.0, Pop
308224 *[LDP/9] 3d 01:16:52, metric 1
 > to 10.10.20.1 via xe-0/0/0.0, Pop
308224(S=0) *[LDP/9] 3d 01:16:52, metric 1
 > to 10.10.20.1 via xe-0/0/0.0, Pop
314736 *[L2IW/6] 02:35:31, metric2 1
 > to 10.10.6.2 via xe-0/1/0.0, Swap 300208
 [L2CKT/7] 02:35:31
 > via iw0.0, Pop Offset: 4
314752 *[L2IW/6] 02:35:31, metric2 1
 > to 10.10.1.1 via xe-0/3/0.0, Swap 301328
 [L2CKT/7] 02:35:47
 > via iw0.1, Pop Offset: 4
iw0.0 *[L2CKT/7] 02:35:31, metric2 1
 > to 10.10.1.1 via xe-0/3/0.0, Push 301328 Offset: -4
iw0.1 *[L2CKT/7] 02:35:47, metric2 1
 > to 10.10.6.2 via xe-0/1/0.0, Push 300208 Offset: -4

```

7. Verify that Router CE1 can send traffic to and receive traffic from Router CE5 across the interconnection, using the **ping** command.

```

user@CE1> ping 198.51.100.11
PING 198.51.100.11 (198.51.100.11): 56 data bytes
64 bytes from 198.51.100.11: icmp_seq=1 ttl=64 time=22.425 ms
64 bytes from 198.51.100.11: icmp_seq=2 ttl=64 time=1.299 ms
64 bytes from 198.51.100.11: icmp_seq=3 ttl=64 time=1.032 ms
64 bytes from 198.51.100.11: icmp_seq=4 ttl=64 time=1.029 ms

```

8. Verify that Router CE5 can send traffic to and receive traffic from Router CE1 across the interconnection, using the **ping** command.

```

user@CE5>ping 198.51.100.1
PING 198.51.100.1 (198.51.100.1): 56 data bytes
64 bytes from 198.51.100.1: icmp_seq=0 ttl=64 time=1.077 ms
64 bytes from 198.51.100.1: icmp_seq=1 ttl=64 time=0.957 ms
64 bytes from 198.51.100.1: icmp_seq=2 ttl=64 time=1.057 ms 1.017 ms

```

## Results

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

The relevant sample configuration for Router PE1 follows.

```

Router PE1 [edit]
interfaces {
 xe-0/1/0 {
 unit 0 {
 family inet {
 address 10.10.2.1/30;
 }
 family mpls;
 }
 }
 xe-0/2/0 {
 unit 0 {
 family inet {
 address 10.10.3.1/30;
 }
 family mpls;
 }
 }
 xe-0/3/0 {
 unit 0 {
 family inet {
 address 10.10.1.1/30;
 }
 family mpls;
 }
 }
 ge-1/0/0 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
 }
 lo0 {
 unit 0 {
 family inet {
 address 192.0.2.1/24;
 }
 }
 }
}
forwarding-options {
 hash-key {
 family inet {

```

```
 layer-3;
 layer-4;
 }
 family mpls {
 label-1;
 label-2;
 }
}
routing-options {
 static {
 route 172.16.0.0/8 next-hop 172.19.59.1;
 }
 autonomous-system 65000;
}
protocols {
 mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 }
 ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 l2circuit {
 neighbor 192.0.2.3 {
 interface ge-1/0/0.0 {
 virtual-circuit-id 100;
 ignore-mtu-mismatch;
 }
 }
 }
}
```

The relevant sample configuration for Router PE3 follows.

```
Router PE3 [edit]
interfaces {
 xe-0/0/0 {
 unit 0 {
 family inet {
 address 10.10.20.2/30;
 }
 }
 }
}
```



```

 family mpls;
 }
}
xe-0/1/0 {
 unit 0 {
 family inet {
 address 10.10.6.1/30;
 }
 family mpls;
 }
}
xe-0/2/0 {
 unit 0 {
 family inet {
 address 10.10.5.2/30;
 }
 family mpls;
 }
}
xe-0/3/0 {
 unit 0 {
 family inet {
 address 10.10.1.2/30;
 }
 family mpls;
 }
}
ge-1/0/1 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
}
iw0 {
 unit 0 {
 encapsulation ethernet-ccc;
 peer-unit 1;
 }
 unit 1 {
 encapsulation ethernet-ccc;
 peer-unit 0;
 }
}
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.3/24;
 }
 }
}
}
routing-options {
 static {
 route 172.16.0.0/8 next-hop 172.19.59.1;
 }
}
autonomous-system 65000;

```

```
}
protocols {
 l2iw;
 mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 ospf {
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 }
 ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 l2circuit {
 neighbor 192.0.2.1 {
 interface iw0.0 {
 virtual-circuit-id 100;
 ignore-mtu-mismatch;
 }
 }
 neighbor 192.0.2.5 {
 interface iw0.1 {
 virtual-circuit-id 200;
 ignore-mtu-mismatch;
 }
 }
 }
}
```

**Related  
Documentation**

- [Applications for Interconnecting a Layer 2 Circuit with a Layer 2 Circuit on page 990](#)

## Applications for Interconnecting a Layer 2 Circuit with a Layer 3 VPN

---

MPLS-based Layer 2 services are growing in demand among enterprise and service providers. This creates new challenges related to interoperability between Layer 2 and Layer 3 services for service providers who want to provide end-to-end value-added services. There are various reasons to stitch different Layer 2 services to one another and to Layer 3 services. For example, to expand the service offerings and to expand geographically. The Junos OS has various features to address the needs of the service provider.

Interconnecting a Layer 2 Circuit with a Layer 3 VPN provides the following benefits:

- Interconnecting a Layer 2 Circuit with a Layer 3 VPN enables the sharing of a service provider's core network infrastructure between IP and Layer 2 circuit services, reducing the cost of providing those services. A Layer 2 MPLS circuit allows service providers to create a Layer 2 circuit service over an existing IP and MPLS backbone.
- Service providers do not have to invest in separate Layer 2 equipment to provide Layer 2 circuit service. A service provider can configure a provider edge router to run any Layer 3 protocol in addition to the Layer 2 protocols. Customers who prefer to maintain control over most of the administration of their own networks want Layer 2 circuit connections with their service provider instead of a Layer 3 VPN connection.

### Related Documentation

- [Understanding Layer 3 VPNs](#)
- [Example: Interconnecting a Layer 2 Circuit with a Layer 3 VPN on page 1015](#)

## Example: Interconnecting a Layer 2 Circuit with a Layer 3 VPN

---

This example provides a step-by-step procedure and commands for configuring and verifying a Layer 2 circuit to Layer 3 VPN interconnection. It contains the following sections:

- [Requirements on page 1015](#)
- [Overview and Topology on page 1016](#)
- [Configuration on page 1017](#)
- [Verifying the Layer 2 Circuit to Layer 3 VPN Interconnection on page 1027](#)

### Requirements

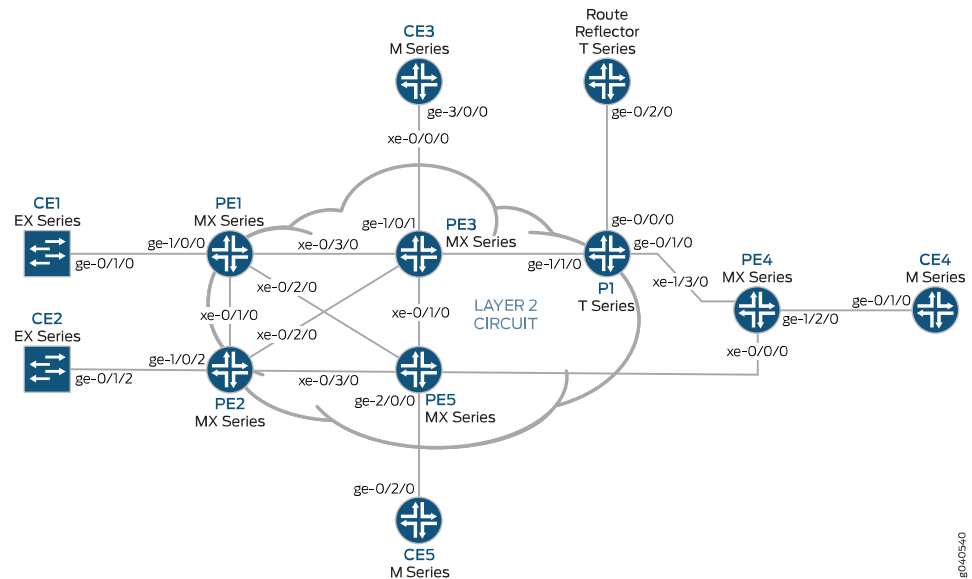
This example uses the following hardware and software components:

- Junos OS Release 9.3 or later
- 3 MX Series 3D Universal Edge Routers
- 1 M Series Multiservice Edge Router
- 1 T Series Core Router
- 1 EX Series Ethernet Switch

## Overview and Topology

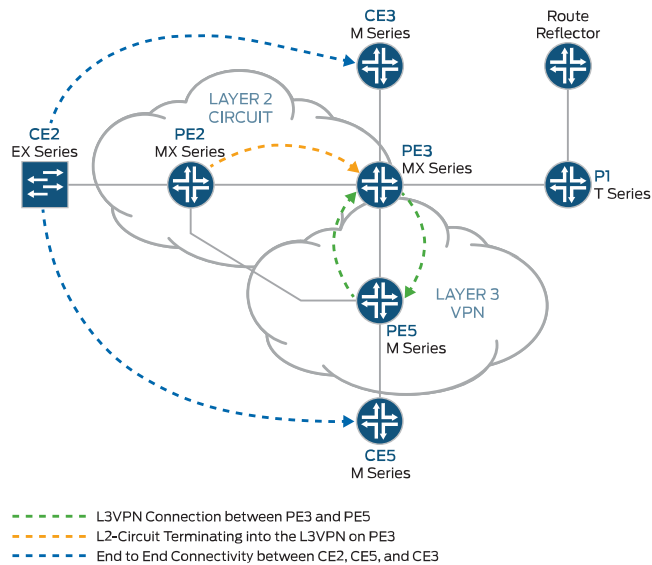
The physical topology of a Layer 2 circuit to Layer 3 VPN interconnection is shown in [Figure 89 on page 1016](#).

**Figure 89: Physical Topology of a Layer 2 Circuit to Layer 3 VPN Interconnection**



The logical topology of a Layer 2 circuit to Layer 3 VPN interconnection is shown in [Figure 90 on page 1016](#).

**Figure 90: Logical Topology of a Layer 2 Circuit to Layer 3 VPN Interconnection**



## Configuration



**NOTE:** In any configuration session, it is good practice to verify periodically 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:

- **CE2** identifies the customer edge 2 (CE2) router
- **PE1** identifies the provider edge 1 (PE1) router
- **CE3** identifies the customer edge 3 (CE3) router
- **PE3** identifies the provider edge 3 (PE3) router
- **CE5** identifies the customer edge 5 (CE5) router
- **PE5** identifies the provider edge 5 (PE5) router

This example contains the following procedures:

- [Configuring PE Router Customer-facing and Loopback Interfaces on page 1017](#)
- [Configuring Core-facing Interfaces on page 1019](#)
- [Configuring Protocols on page 1020](#)
- [Configuring Routing Instances and Layer 2 Circuits on page 1023](#)
- [Configuring the Route Reflector on page 1025](#)
- [Interconnecting the Layer 2 Circuit with the Layer 3 VPN on page 1026](#)

### Configuring PE Router Customer-facing and Loopback Interfaces

#### Step-by-Step Procedure

To begin building the interconnection, configure the interfaces on the PE routers. If your network contains provider (P) routers, configure the interfaces on the P routers also. This example shows the configuration for Router PE2, Router PE3, and Router PE5.

1. On Router PE2, configure the **ge-1/0/2** interface encapsulation. To configure the interface encapsulation, include the **encapsulation** statement and specify the **ethernet-ccc** option (**vlan-ccc** encapsulation is also supported). Configure the **ge-1/0/2.0** logical interface family for circuit cross-connect functionality. To configure the logical interface family, include the **family** statement and specify the **ccc** option. The encapsulation should be configured the same way for all routers in the Layer 2 circuit domain.

```
[edit interfaces]
ge-1/0/2 {
 encapsulation ethernet-ccc;
 unit 0 {
 family ccc;
 }
}
```

2. On Router PE2, configure the **lo0.0** interface. Include the **family** statement and specify the **inet** option. Include the **address** statement and specify **192.0.2.2/24** as the loopback IPv4 address.

```
[edit interfaces]
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.2/24;
 }
 }
}
```

3. On Router PE3, configure the **ge-1/0/1** interface. Include the **family** statement and specify the **inet** option. Include the **address** statement and specify **198.51.100.1/24** as the interface address for this device.

```
[edit interfaces]
ge-1/0/1 {
 unit 0 {
 family inet {
 address 198.51.100.1/24;
 }
 }
}
```

4. On Router PE3, configure the **lo0.0** loopback interface. Include the **family** statement and specify the **inet** option. Include the **address** statement and specify **192.0.2.3/24** as the loopback IPv4 address for this router.

```
[edit interfaces]
lo0 {
 unit 0 {
 family inet {
 address 192.0.2.3/24;
 }
 }
}
```

5. On Router PE5, configure the **ge-2/0/0** interface. Include the **family** statement and specify the **inet** option. Include the **address** statement and specify **198.51.100.8/24** as the interface address.

```
[edit interfaces]
ge-2/0/0 {
 unit 0 {
 family inet {
 address 198.51.100.8/24;
 }
 }
}
```

6. On Router PE5, configure the **lo0.0** interface. Include the **family** statement and specify the **inet** option. Include the **address** statement and specify **192.0.2.5/24** as the loopback IPv4 address for this router.

```
[edit interfaces]
lo0 {
```

```

 unit 0 {
 family inet {
 address 192.0.2.5/24;
 }
 }
}

```

### Configuring Core-facing Interfaces

#### Step-by-Step Procedure

This procedure describes how to configure the core-facing interfaces on the PE routers. This example does not include all the core-facing interfaces shown in the physical topology illustration. Enable the **mpls** and **inet** address families on the core-facing interfaces.

1. On Router PE2, configure the **xe-0/2/0** interface. Include the **family** statement and specify the **inet** address family. Include the **address** statement and specify **10.10.5.1/30** as the interface address. Include the **family** statement and specify the **mpls** address family.

```

[edit interfaces]
xe-0/2/0 {
 unit 0 {
 family inet {
 address 10.10.5.1/30;
 }
 family mpls;
 }
}

```

2. On Router PE3, configure the core-facing interfaces. Include the **family** statement and specify the **inet** address family. Include the **address** statement and specify the IPv4 addresses shown in the example as the interface addresses. Include the **family** statement and specify the **mpls** address family. In the example, the **xe-2/1/0** interface is connected to Router PE5, and the **xe-2/2/0** interface is connected to Router PE2.

```

[edit interfaces]
xe-2/0/0 {
 unit 0 {
 family inet {
 address 10.10.20.2/30;
 }
 family mpls;
 }
}
xe-2/1/0 {
 unit 0 {
 family inet {
 address 10.10.6.1/30;
 }
 family mpls;
 }
}
xe-2/2/0 {
 unit 0 {
 family inet {

```

```

 address 10.10.5.2/30;
 }
 family mpls;
}
}
xe-2/3/0 {
 unit 0 {
 family inet {
 address 10.10.1.2/30;
 }
 family mpls;
 }
}

```

3. On Router PE5, configure the **xe-0/1/0** interface. Include the **family** statement and specify the **inet** address family. Include the **address** statement and specify **10.10.6.2/30** as the interface address. Include the **family** statement and specify the **mpls** address family.

```

[edit interfaces]
xe-0/1/0 {
 unit 0 {
 family inet {
 address 10.10.6.2/30;
 }
 family mpls;
 }
}

```

### Configuring Protocols

#### Step-by-Step Procedure

This procedure describes how to configure the protocols used in this example. If your network contains P routers, configure the interfaces on the P routers also.

1. On Router PE3, enable OSPF as the IGP. Enable the MPLS, LDP, and BGP protocols on all interfaces except **fxp0.0**. LDP is used as the signaling protocol for the Layer 2 circuit to Router PE2. The following configuration snippet shows the protocol configuration for Router PE3:

```

[edit]
protocols {
 rsvp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 mpls {
 label-switched-path to-RR {
 to 192.0.2.7;
 }
 label-switched-path to-PE2 {
 to 192.0.2.2;
 }
 label-switched-path to-PE5 {

```



```

 to 192.0.2.5;
 }
 label-switched-path to-PE4 {
 to 192.0.2.4;
 }
 label-switched-path to-PE1 {
 to 192.0.2.1;
 }
 interface all;
 interface fxp0.0 {
 disable;
 }
}
bgp {
 group RR {
 type internal;
 local-address 192.0.2.3;
 family inet-vpn {
 unicast;
 }
 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
}
ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}
ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
}
}

```

2. On Router PE2, configure the MPLS, OSPF, and LDP protocols.

```

[edit]
protocols {
 mpls {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {

```

```

 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}
ldp {
 interface all;
 interface fxp0.0 {
 disable;
 }
}
}

```

3. On Router PE5, enable OSPF as the IGP. Enable the MPLS, RSVP, and BGP protocols on all interfaces except **fxp0.0**. Enable core-facing interfaces with the **mpls** and **inet** address families.

```

[edit]
protocols {
 rsvp {
 interface all {
 link-protection;
 }
 interface fxp0.0 {
 disable;
 }
 }
 mpls {
 label-switched-path to-RR {
 to 192.0.2.7;
 }
 label-switched-path to-PE2 {
 to 192.0.2.2;
 }
 label-switched-path to-PE3 {
 to 192.0.2.3;
 }
 label-switched-path to-PE4 {
 to 192.0.2.4;
 }
 label-switched-path to-PE1 {
 to 192.0.2.1;
 }
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}
bgp {
 group to-rr {
 type internal;
 local-address 192.0.2.5;
 family inet-vpn {
 unicast;
 }
 }
}

```

```

 family l2vpn {
 signaling;
 }
 neighbor 192.0.2.7;
 }
}
ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
}
}
}

```

### Configuring Routing Instances and Layer 2 Circuits

#### Step-by-Step Procedure

This procedure describes how to configure the Layer 2 circuit and the Layer 3 VPN.

1. On Router PE2, configure the Layer 2 circuit. Include the **l2circuit** statement. Include the **neighbor** statement and specify the loopback IPv4 address of Router PE3 as the neighbor. Include the interface statement and specify **ge-1/0/2.0** as the logical interface that is participating in the Layer 2 circuit. Include the **virtual-circuit-id** statement and specify **100** as the identifier. Include the **no-control-word** statement for equipment that does not support the control word.

```

[edit]
protocols {
 l2circuit {
 neighbor 192.0.2.3 {
 interface ge-1/0/2.0 {
 virtual-circuit-id 100;
 no-control-word;
 }
 }
 }
}
}

```

2. On Router PE3, configure the Layer 2 circuit to Router PE2. Include the **l2circuit** statement. Include the **neighbor** statement and specify the loopback IPv4 address of Router PE2 as the neighbor. Include the interface statement and specify **lt-1/1/10.0** as the logical tunnel interface that is participating in the Layer 2 circuit. Include the **virtual-circuit-id** statement and specify **100** as the identifier. Include the **no-control-word** statement.

```

[edit]
protocols {
 l2circuit {
 neighbor 192.0.2.2 {
 interface lt-1/1/10.0 {
 virtual-circuit-id 100;
 no-control-word;
 }
 }
 }
}

```

```
 }
 }
}
```

3. On Router PE3, configure the Layer 3 VPN (**L3VPN**) routing instance to Router PE5 at the **[edit routing-instances]** hierarchy level. Also configure the BGP peer group at the **[edit routing-instances L3VPN protocols]** hierarchy level.

```
[edit]
routing-instances {
 L3VPN {
 instance-type vrf;
 interface ge-1/0/1.0;
 interface lt-1/1/10.1;
 route-distinguisher 65000:33;
 vrf-target target:65000:2;
 vrf-table-label;
 protocols {
 bgp {
 export direct;
 group ce3 {
 neighbor 198.51.100.6 {
 peer-as 100;
 }
 }
 }
 }
 }
}
```

4. On Router PE5, configure the Layer 3 VPN routing instance (**L3VPN**) at the **[edit routing-instances]** hierarchy level. Also configure the BGP peer group at the **[edit routing-instances L3VPN protocols]** hierarchy level.

```
[edit]
routing-instances {
 L3VPN {
 instance-type vrf;
 interface ge-2/0/0.0;
 route-distinguisher 65000:5;
 vrf-target target:65000:2;
 vrf-table-label;
 protocols {
 bgp {
 group ce5 {
 neighbor 198.51.100.10 {
 peer-as 200;
 }
 }
 }
 }
 }
}
```

### Configuring the Route Reflector

**Step-by-Step Procedure** Although a route reflector is not required to interconnect a Layer 2 circuit with a Layer 3 VPN, this examples uses a route reflector. This procedure shows the relevant portion of the route reflector configuration.

1. Configure the route reflector with RSVP, MPLS, BGP and OSPF. The route reflector is a BGP peer with the PE routers. Notice that the BGP peer group configuration includes the **family** statement and specifies the **inet-vpn** option. The **inet-vpn** option enables BGP to advertise network layer reachability information (NLRI) for the Layer 3 VPN routes. The configuration also includes the **family** statement and specifies the **l2vpn** option. The **l2vpn** option enables BGP to advertise NLRI for the Layer 2 circuit. Layer 2 circuits use the same internal BGP infrastructure as Layer 2 VPNs.

```
[edit]
protocols {
 rsvp {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 mpls {
 label-switched-path to-pe3 {
 to 192.0.2.3;
 }
 label-switched-path to-pe5 {
 to 192.0.2.5;
 }
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 bgp {
 group RR {
 type internal;
 local-address 192.0.2.7;
 family inet {
 unicast;
 }
 family inet-vpn {
 unicast;
 }
 family l2vpn {
 signaling;
 }
 cluster 192.0.2.7;
 neighbor 192.0.2.1;
 neighbor 192.0.2.2;
 neighbor 192.0.2.4;
 neighbor 192.0.2.5;
 neighbor 192.0.2.3;
 }
 }
}
```

```

 }
 ospf {
 traffic-engineering;
 area 0.0.0.0 {
 interface all;
 interface fxp0.0 {
 disable;
 }
 }
 }
}

```

### Interconnecting the Layer 2 Circuit with the Layer 3 VPN

#### Step-by-Step Procedure

Before you can configure the logical tunnel interface in an MX Series router, you must create the tunnel services interface to be used for tunnel services.

1. Create the tunnel service interface on Router PE3. Include the **bandwidth** statement at the **[edit chassis fpc slot-number pic slot-number tunnel-services]** hierarchy level and specify the amount of bandwidth to reserve for tunnel services in gigabits per second.

```

[edit chassis]
fpc 1 {
 pic 1 {
 tunnel-services {
 bandwidth 1g;
 }
 }
}

```

2. On Router PE3, configure the **lt-1/1/10** logical tunnel interface unit 0.

Router PE3 is the router that is *stitching* the Layer 2 circuit to the Layer 3 VPN using the logical tunnel interface. The configuration of the peer unit interfaces is what makes the interconnection.

Include the **encapsulation** statement and specify the **ethernet-ccc** option. Include the **peer-unit** statement and specify the logical interface unit 1 as the peer tunnel interface. Include the **family** statement and specify the **ccc** option.

Configure the **lt-1/1/10** logical interface unit 1 with **ethernet** encapsulation. Include the **peer-unit** statement and specify the logical interface unit 0 as the peer tunnel interface. Include the **family** statement and specify the **inet** option. Also include the **address** statement and specify **198.51.100.11/24** as the IPv4 address of the interface.



**NOTE:** The peering logical interfaces must belong to the same logical tunnel interface derived from the Tunnel Services PIC.

```

[edit interfaces]
lt-1/1/10 {
 unit 0 {

```

```

 encapsulation ethernet-ccc;
 peer-unit 1;
 family ccc;
 }
 unit 1 {
 encapsulation ethernet;
 peer-unit 0;
 family inet {
 address 198.51.100.11/24;
 }
 }
}

```

3. On each router, commit the configuration.

```

user@host> commit check
configuration check succeeds
user@host> commit

```

## Verifying the Layer 2 Circuit to Layer 3 VPN Interconnection

To verify that the interconnection is working properly, perform these tasks:

- [Verifying That the Layer 2 Circuit Connection to Router PE3 is Up on page 1027](#)
- [Verifying LDP Neighbors and Targeted LDP LSPs on Router PE2 on page 1028](#)
- [Verifying the Layer 2 Circuit Routes on Router PE2 on page 1028](#)
- [Verifying That the Layer 2 Circuit Connection to Router PE2 is Up on page 1029](#)
- [Verifying LDP Neighbors and Targeted LDP LSPs on Router PE3 on page 1030](#)
- [Verifying a BGP Peer Session with the Route Reflector on Router PE3 on page 1030](#)
- [Verifying the Layer 3 VPN Routes on Router PE3 on page 1031](#)
- [Verifying the Layer 2 Circuit Routes on Router PE3 on page 1031](#)
- [Verifying the MPLS Routes on Router PE3 on page 1032](#)
- [Verifying Traffic Flow Between Router CE2 and Router CE3 on page 1033](#)
- [Verifying Traffic Flow Between Router CE2 and Router CE5 on page 1033](#)

### Verifying That the Layer 2 Circuit Connection to Router PE3 is Up

**Purpose** To verify that the Layer 2 circuit connection from Router PE2 to Router PE3 is **Up**. To also document the incoming and outgoing LDP labels and the circuit ID used by this Layer 2 circuit connection.

**Action** Verify that the Layer 2 circuit connection is up, using the **show l2circuit connections** command.

```
user@PE2> show l2circuit connections
```

Legend for connection status (St)

|                              |                                 |
|------------------------------|---------------------------------|
| EI -- encapsulation invalid  | NP -- interface h/w not present |
| MM -- mtu mismatch           | Dn -- down                      |
| EM -- encapsulation mismatch | VC-Dn -- Virtual circuit Down   |
| CM -- control-word mismatch  | Up -- operational               |

VM -- vlan id mismatch                      CF -- Call admission control failure  
 OL -- no outgoing label                      IB -- TDM incompatible bitrate  
 NC -- intf encaps not CCC/TCC              TM -- TDM misconfiguration  
 BK -- Backup Connection                    ST -- Standby Connection  
 CB -- rcvd cell-bundle size bad           SP -- Static Pseudowire  
 LD -- local site signaled down           RS -- remote site standby  
 RD -- remote site signaled down          XX -- unknown

#### Legend for interface status

Up -- operational

Dn -- down

Neighbor: 192.0.2.3

| Interface          | Type | St | Time last up        | # Up trans |
|--------------------|------|----|---------------------|------------|
| ge-1/0/2.0(vc 100) | rmt  | Up | Jan 7 02:14:13 2010 | 1          |

Remote PE: 192.0.2.3, Negotiated control-word: No  
 Incoming label: 301488, Outgoing label: 315264  
 Negotiated PW status TLV: No  
 Local interface: ge-1/0/2.0, Status: Up, Encapsulation: ETHERNET

**Meaning** The output shows that the Layer 2 circuit connection from Router PE2 to Router PE3 is **Up** and the connection is using the **ge-1/0/2.0** interface. Note that the outgoing label is **315264** and the incoming label is **301488**, the virtual circuit (VC) identifier is **100** and the encapsulation is **ETHERNET**.

#### Verifying LDP Neighbors and Targeted LDP LSPs on Router PE2

**Purpose** To verify that Router PE2 has a targeted LDP LSP to Router PE3 and that Router PE2 and Router PE3 are LDP neighbors.

**Action** Verify that Router PE2 has a targeted LDP LSP to Router PE3 and that Router PE2 and Router PE3 are LDP neighbors, using the **show ldp neighbor** command.

```

user@PE2> show ldp neighbor
Address Interface Label space ID Hold time
192.0.2.3 lo0.0 192.0.2.3:0 38

```

**Meaning** The output shows that Router PE2 has an LDP neighbor with the IPv4 address of **192.0.2.3**. Address 192.0.2.3 is the lo0.0 interface address of Router PE3. Notice that Router PE2 uses the local **lo0.0** interface for the LSP.

Verifying that the routers are LDP neighbors also verifies that the targeted LSP is established.

#### Verifying the Layer 2 Circuit Routes on Router PE2

**Purpose** To verify that Router PE2 has a route for the Layer 2 circuit and that the route uses the LDP MPLS label to Router PE3.

**Action** Verify that Router PE2 has a route for the Layer 2 circuit and that the route uses the LDP MPLS label to Router PE3, using the **show route table mpls.0** command.

```

user@PE2> show route table mpls.0
mpls.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

```



```

0 *[MPLS/0] 1w3d 05:24:11, metric 1
 Receive
1 *[MPLS/0] 1w3d 05:24:11, metric 1
 Receive
2 *[MPLS/0] 1w3d 05:24:11, metric 1
 Receive
300560 *[LDP/9] 16:12:23, metric 1
 > to 10.10.2.1 via xe-0/1/0.0, Pop
300560(S=0) *[LDP/9] 16:12:23, metric 1
 > to 10.10.2.1 via xe-0/1/0.0, Pop
301008 *[LDP/9] 16:12:23, metric 1
 > to 10.10.4.2 via xe-0/3/0.0, Swap 299856
301488 *[L2CKT/7] 11:07:28
 > via ge-1/0/2.0, Pop
301536 *[LDP/9] 16:12:23, metric 1
 > to 10.10.4.2 via xe-0/3/0.0, Pop
301536(S=0) *[LDP/9] 16:12:23, metric 1
 > to 10.10.4.2 via xe-0/3/0.0, Pop
301712 *[LDP/9] 12:41:22, metric 1
 > to 10.10.5.2 via xe-0/2/0.0, Swap 315184
301728 *[LDP/9] 12:41:22, metric 1
 > to 10.10.5.2 via xe-0/2/0.0, Pop
301728(S=0) *[LDP/9] 12:41:22, metric 1
 > to 10.10.5.2 via xe-0/2/0.0, Pop
ge-1/0/2.0 *[L2CKT/7] 11:07:28, metric2 1
 > to 10.10.5.2 via xe-0/2/0.0, Push 315264

```

**Meaning** The output shows that Router PE2 pushes the **315264** outgoing label on the **L2CKT** route going out interface **ge-1/0/2.0**. The output also shows that Router PE2 pops the **301488** incoming label on the **L2CKT** coming from interface **ge-1/0/2.0**

### Verifying That the Layer 2 Circuit Connection to Router PE2 is Up

**Purpose** To verify that the Layer 2 circuit connection from Router PE3 to Router PE2 is **Up**, To also document the incoming and outgoing LDP labels and the circuit ID used by this Layer 2 circuit connection.

**Action** Verify that the Layer 2 circuit connection is up, using the **show l2circuit connections** command.

```
user@PE3> show l2circuit connections
```

Layer-2 Circuit Connections:

Legend for connection status (St)

|                                 |                                      |
|---------------------------------|--------------------------------------|
| EI -- encapsulation invalid     | NP -- interface h/w not present      |
| MM -- mtu mismatch              | Dn -- down                           |
| EM -- encapsulation mismatch    | VC-Dn -- Virtual circuit Down        |
| CM -- control-word mismatch     | Up -- operational                    |
| VM -- vlan id mismatch          | CF -- Call admission control failure |
| OL -- no outgoing label         | IB -- TDM incompatible bitrate       |
| NC -- intf encaps not CCC/TCC   | TM -- TDM misconfiguration           |
| BK -- Backup Connection         | ST -- Standby Connection             |
| CB -- rcvd cell-bundle size bad | XX -- unknown                        |

Legend for interface status

Up -- operational

Dn -- down

Neighbor: 192.0.2.2

```

Interface Type St Time last up # Up trans
lt-1/1/10.0(vc 100) rmt Up Jan 7 02:15:03 2010 1
Remote PE: 192.0.2.2, Negotiated control-word: No
Incoming label: 315264, Outgoing label: 301488
Local interface: lt-1/1/10.0, Status: Up, Encapsulation: ETHERNET

```

**Meaning** The output shows that the Layer 2 circuit connection from Router PE3 to Router PE2 is **Up** and the connection is using the logical tunnel (lt) interface. Note that the incoming label is **315264** and the outgoing label is **301488**, the virtual circuit (VC) identifier is **100**, and that the encapsulation is **ETHERNET**.

### Verifying LDP Neighbors and Targeted LDP LSPs on Router PE3

**Purpose** To verify that Router PE3 has a targeted LDP LSP to Router PE2 and that Router PE3 and Router PE2 are LDP neighbors.

**Action** Verify that Router PE2 has a targeted LDP LSP to Router PE3 and that Router PE2 and Router PE3 are LDP neighbors, using the **show ldp neighbor** command.

```

user@PE2> show ldp neighbor
Address Interface Label space ID Hold time
192.0.2.2 lo0.0 192.0.2.2:0 43
192.0.2.4 lo0.0 192.0.2.4:0 33

```

**Meaning** The output shows that Router PE3 has an LDP neighbor with the IPv4 address of **192.0.2.2**. Address 192.0.2.2 is the lo0.0 interface address of Router PE2. The output also shows that the interface used on Router PE3 for the LSP is **lo0.0**. Verifying that the routers are LDP neighbors also verifies that the targeted LSP is established.

### Verifying a BGP Peer Session with the Route Reflector on Router PE3

**Purpose** To verify that Router PE3 has a peer session established with the route reflector.

**Action** Verify that Router PE3 has a peer session established with the route reflector, using the **show bgp summary** command.

```
user@PE2> show bgp summary
```

```

Groups: 2 Peers: 2 Down peers: 0
Table Tot Paths Act Paths Suppressed History Damp State Pending
bgp.13vpn.0 1 1 0 0 0 0 0
Peer AS InPkt OutPkt OutQ Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
192.0.2.7 65000 1597 1612 0 1 12:03:21 Establ
 bgp.12vpn.0: 0/0/0/0
 bgp.13vpn.0: 1/1/1/0
 L3VPN.inet.0: 1/1/1/0

```

**Meaning** The output shows that Router PE3 has a peer session with the router with the IPv4 address of **192.0.2.7**. Address 192.0.2.7 is the lo0.0 interface address of the route reflector. The output also shows that the peer session state is **Establ**, meaning that the session is established.

### Verifying the Layer 3 VPN Routes on Router PE3

**Purpose** To verify that Router PE3 has Layer 3 VPN routes to Router CE2, Router CE3, and Router CE5.

**Action** Verify that Router PE3 has routes to Router CE2, Router CE3, and Router CE5 in the Layer 3 VPN route table, using the **show route table L3VPN.inet.0** command. In this example, **L3VPN** is the name configured for the routing instance.

```
user@PE3> show route table L3VPN.inet.0
L3VPN.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

198.51.100.10/24 *[Direct/0] 11:13:59
 > via lt-1/1/10.1
198.51.100.11/24 *[Local/0] 11:13:59
 Local via lt-1/1/10.1
198.51.100.12/24 *[BGP/170] 11:00:41, localpref 100, from 192.0.2.7
 AS path: I
 > to 10.10.6.2 via xe-2/1/0.0, Push 16
198.51.100.13/24 *[Direct/0] 11:54:41
 > via ge-1/0/1.0
198.51.100.1/24 *[Local/0] 11:54:41
 Local via ge-1/0/1.0
```

**Meaning** The output shows that Router PE3 has a route to the IPv4 subnetwork address of **198.51.100.10**. Address 198.51.100.15 is the interface address of Router CE2. The output shows that Router PE3 has a route to the IPv4 subnetwork address of **198.51.100.11**. Address 198.51.100.10 is the interface address of Router CE5. The output shows that Router PE3 has a route to the IPv4 subnetwork address of **198.51.100.13**. Address 198.51.100.6 is the interface address of Router CE3.

### Verifying the Layer 2 Circuit Routes on Router PE3

**Purpose** To verify that Router PE3 has a route to Router PE2 in the Layer 2 circuit route table.

**Action** Verify that Router PE3 has a route to Router PE2 in the Layer 2 circuit route table, using the **show route table l2circuit.0** command.

```
user@PE3> show route table l2circuit.0
192.0.2.2:NoCtrlWord:5:100:Local/96 (1 entry, 1 announced)
 *L2CKT Preference: 7
 Next hop type: Indirect
 Next-hop reference count: 1
 Next hop type: Router
 Next hop: 10.10.5.1 via xe-2/2/0.0, selected
 Protocol next hop: 192.0.2.2
 Indirect next hop: 8cae0a0 -
 State: <Active Int>
 Local AS: 65000
 Age: 11:16:50 Metric2: 1
 Task: l2 circuit
 Announcement bits (1): 0-LDP
 AS path: I
 VC Label 315264, MTU 1500
```

**Meaning** The output shows that Router PE3 has a route to the IPv4 address of **192.0.2.2**. Address 192.0.2.2 is the lo0.0 interface address of Router PE2. Note that the VC label is **315264**. This label is the same as the incoming MPLS label displayed using the **show l2circuit connections** command.

### Verifying the MPLS Routes on Router PE3

**Purpose** To verify that Router PE3 has a route to Router PE2 in the MPLS route table.

**Action** Verify Router PE3 has a route to Router PE2 in the MPLS route table, using the **show route table mpls.0** command.

```
user@PE3> show route table mpls.0
mpls.0: 21 destinations, 21 routes (21 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0 *[MPLS/0] 1w3d 05:29:02, metric 1
 Receive
1 *[MPLS/0] 1w3d 05:29:02, metric 1
 Receive
2 *[MPLS/0] 1w3d 05:29:02, metric 1
 Receive
16 *[VPN/0] 12:22:45
 to table L3VPN.inet.0, Pop
315184 *[LDP/9] 12:45:14, metric 1
 > to 10.10.20.1 via xe-2/0/0.0, Pop
315184(S=0) *[LDP/9] 12:45:14, metric 1
 > to 10.10.20.1 via xe-2/0/0.0, Pop
315200 *[LDP/9] 00:03:53, metric 1
 > to 10.10.20.1 via xe-2/0/0.0, Swap 625297
 to 10.10.6.2 via xe-2/1/0.0, Swap 299856
315216 *[LDP/9] 12:45:14, metric 1
 > to 10.10.6.2 via xe-2/1/0.0, Pop
315216(S=0) *[LDP/9] 12:45:14, metric 1
 > to 10.10.6.2 via xe-2/1/0.0, Pop
315232 *[LDP/9] 12:45:06, metric 1
 > to 10.10.1.1 via xe-2/3/0.0, Pop
315232(S=0) *[LDP/9] 12:45:06, metric 1
 > to 10.10.1.1 via xe-2/3/0.0, Pop
315248 *[LDP/9] 12:45:14, metric 1
 > to 10.10.5.1 via xe-2/2/0.0, Pop
315248(S=0) *[LDP/9] 12:45:14, metric 1
 > to 10.10.5.1 via xe-2/2/0.0, Pop
315264 *[L2CKT/7] 11:11:20
 > via lt-1/1/10.0, Pop
315312 *[RSVP/7] 11:26:01, metric 1
 > to 10.10.6.2 via xe-2/1/0.0, label-switched-path to-pe5
315312(S=0) *[RSVP/7] 11:26:01, metric 1
 > to 10.10.6.2 via xe-2/1/0.0, label-switched-path to-pe5
315328 *[RSVP/7] 11:26:01, metric 1
 > to 10.10.20.1 via xe-2/0/0.0, label-switched-path to-RR
315360 *[RSVP/7] 11:26:01, metric 1
 > to 10.10.20.1 via xe-2/0/0.0, label-switched-path to-RR
316208 *[RSVP/7] 00:03:32, metric 1
 > to 10.10.6.2 via xe-2/1/0.0, label-switched-path
Bypass->10.10.9.1
316208(S=0) *[RSVP/7] 00:03:32, metric 1
 > to 10.10.6.2 via xe-2/1/0.0, label-switched-path
```

```

Bypass->10.10.9.1
lt-1/1/10.0 *[L2CKT/7] 11:11:20, metric2 1
 > to 10.10.5.1 via xe-2/2/0.0, Push 301488

```

**Meaning** The output shows that Router PE3 has a route for the Layer 2 circuit and that the route uses the LDP MPLS label to Router PE2. Notice that the **301488** label is the same as the outgoing label displayed on Router PE2 using the **show l2circuit connections** command.

### Verifying Traffic Flow Between Router CE2 and Router CE3

**Purpose** To verify that the CE routers can send and receive traffic across the interconnection.

**Action** Verify that Router CE2 can send traffic to and receive traffic from Router CE3 across the interconnection, using the **ping** command.

```

user@CE2>ping 198.51.100.6
PING 198.51.100.6 (198.51.100.6): 56 data bytes
64 bytes from 198.51.100.6: icmp_seq=0 ttl=63 time=0.708 ms
64 bytes from 198.51.100.6: icmp_seq=1 ttl=63 time=0.610 ms

```

**Meaning** The output shows that Router CE2 can send an ICMP request to and receive a response from Router CE3 across the interconnection.

### Verifying Traffic Flow Between Router CE2 and Router CE5

**Purpose** To verify that the CE routers can send and receive traffic across the interconnection.

**Action** Verify that Router CE2 can send traffic to and receive traffic from Router CE5 across the interconnection, using the **ping** command.

```

user@CE2>ping 198.51.100.10
PING 198.51.100.10 (198.51.100.10): 56 data bytes
64 bytes from 198.51.100.10: icmp_seq=0 ttl=62 time=0.995 ms
64 bytes from 198.51.100.10: icmp_seq=1 ttl=62 time=1.005 ms

```

**Meaning** The output shows that Router CE2 can send an ICMP request to and receive a response from Router CE5 across the interconnection.

**Related Documentation**

- *Understanding Layer 3 VPNs*
- [Applications for Interconnecting a Layer 2 Circuit with a Layer 3 VPN on page 1015](#)



## PART 9

# Configuration Statements and Operational Commands

- [Configuration Statements \(All VPNs\) on page 1037](#)
- [Configuration Statements \(Layer 2 VPNs and VPLS\) on page 1065](#)
- [Operational Commands on page 1233](#)





## CHAPTER 46

# Configuration Statements (All VPNs)


- [aggregate-label](#) on page 1038
- [backup-neighbor](#) on page 1039
- [description \(Routing Instances\)](#) on page 1040
- [family route-target](#) on page 1041
- [graceful-restart \(Enabling Globally\)](#) on page 1042
- [instance-type](#) on page 1044
- [interface \(Routing Instances\)](#) on page 1046
- [no-forwarding](#) on page 1047
- [proxy-generate](#) on page 1048
- [revert-time \(Protocols Layer 2 Circuits\)](#) on page 1049
- [route-distinguisher](#) on page 1051
- [route-distinguisher-id](#) on page 1053
- [route-target-filter](#) on page 1054
- [rtf-prefix-list](#) on page 1055
- [switchover-delay](#) on page 1056
- [unicast-reverse-path](#) on page 1057
- [vpn-apply-export](#) on page 1058
- [vrf-export](#) on page 1059
- [vrf-import](#) on page 1060
- [vrf-mtu-check](#) on page 1061
- [vrf-target](#) on page 1062

## aggregate-label

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>aggregate-label {<br/>    community <i>community-name</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols bgp family inet labeled-unicast],<br>[edit logical-systems <i>logical-system-name</i> protocols bgp family inet6 labeled-unicast],<br>[edit logical-systems <i>logical-system-name</i> protocols bgp family inet-vpn unicast],<br>[edit logical-systems <i>logical-system-name</i> protocols bgp family inet-vpn6 unicast],<br>[edit protocols bgp family inet labeled-unicast],<br>[edit protocols bgp family inet6 labeled-unicast],<br>[edit protocols bgp family inet-vpn unicast],<br>[edit protocols bgp family inet6-vpn unicast] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | Specify matching criteria (in the form of a community) such that all routes which match are assigned the same VPN label, selected from one of the several routes in the set defined by this criteria. This reduces the number of VPN labels that the router must consider, and aggregates the received labels.                                                                                                                                                                                                                                                                                      |
| <b>Options</b>                  | <b>community <i>community-name</i></b> —Specify the name of the community to which to apply the aggregate label.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Aggregate Labels for VPNs on page 21</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## backup-neighbor

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> backup-neighbor address {     community name;     mtu number;     hot-standby;     psn-tunnel-endpoint address;     standby;     static;     virtual-circuit-id number; } </pre>                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | <pre> [edit logical-systems logical-system-name protocols l2circuit local-switching interface interface-name], [edit logical-systems logical-system-name protocols l2circuit neighbor address interface interface-name], [edit logical-systems logical-system-name routing-instances routing-instance-name protocols vpls neighbor address], [edit protocols l2circuit local-switching interface interface-name], [edit protocols l2circuit neighbor address interface interface-name], [edit routing-instances routing-instance-name protocols vpls neighbor address] </pre> |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.2.</p> <p>Statement introduced in Junos OS Release 12.2 for ACX Series routers.</p> <p>Statement introduced in Junos OS Release 12.3 at the <b>[edit protocols l2circuit local-switching interface interface-name]</b> hierarchy level.</p>                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | <p>Configure pseudowire redundancy for Layer 2 circuits and VPLS. A redundant pseudowire can act as a backup connection and can be configured between a PE router and a CE device or between PE routers, maintaining Layer 2 circuit and VPLS services after certain types of failures. This feature can help improve the reliability of certain types of networks where a single point of failure could interrupt service for customers.</p>                                                                                                                                 |
|                                 | <div>  <p><b>NOTE:</b> VPLS is not supported on ACX Series routers. The <b>psn-tunnel-endpoint</b> statement is not supported at the <b>[edit protocols l2circuit local-switching interface interface-name end-interface interface interface-name]</b> hierarchy level.</p> </div>                                                                                                                                                                                                         |
| <b>Options</b>                  | <p><b>address</b>—Specifies the address for the backup neighbor.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Pseudowire Redundancy on the PE Router on page 180</a></li> <li>• <a href="#">Example: Configuring Layer 2 Circuit Switching Protection on page 420</a></li> <li>• <a href="#">community (Protocols Layer 2 Circuit) on page 1078</a></li> </ul>                                                                                                                                                                                                                                                             |

- [psn-tunnel-endpoint on page 1188](#)
- [virtual-circuit-id on page 1222](#)

---

## description (Routing Instances)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | description text;                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> ]                                                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 11.1 for EX Series switches.<br>Statement introduced in Junos OS Release 11.3 for the QFX Series.<br>Statement introduced in Junos OS Release 12.3 for ACX Series routers.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Provide a text description for the routing instance. If the text includes one or more spaces, enclose it in quotation marks (" "). Any descriptive text you include is displayed in the output of the <b>show route instance detail</b> command and has no effect on the operation of the routing instance.                                          |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Description on page 10</a></li><li>• <i>show route instance</i></li></ul>                                                                                                                                                                                                        |

## family route-target

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>family route-target {     advertise-default;     external-paths <i>number</i>;     prefix-limit <i>number</i>;     proxy-generate &lt;route-target-policy <i>route-target-policy-name</i>&gt;; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | <pre>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i>], [edit protocols bgp group <i>group-name</i>], [edit protocols bgp group <i>group-name</i> neighbor <i>address</i>]</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | <p>Enable BGP route target filtering on the VPN.</p> <p>The <b>family route-target</b> statement is useful for filtering VPN routes before they are sent. Provider edge (PE) routers inform the route reflector (RR) which routes to send, using <b>family route-target</b> to provide the route-target-interest information. The RR then sends to the PE router only the advertisements containing the specified route target.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <p><b>advertise-default</b>—Cause the router to advertise the default route target route (0:0:0/0) and suppress all routes that are more specific. This can be used by a route reflector on BGP groups consisting of neighbors that act as provider edge (PE) routers only. PE routers often need to advertise all routes to the route reflector. Suppressing all route target advertisements other than the default route reduces the amount of information exchanged between the route reflector and the PE routers. The Junos OS further helps to reduce route target advertisement overhead by not maintaining dependency information unless a nondefault route is received.</p> <p><b>external-paths <i>number</i></b>—Cause the router to advertise the VPN routes that reference a given route target. The number you specify with the <b>external-paths</b> statement determines the number of external peer routers (currently advertising that route target) that receive the VPN routes. The default value is 1.</p> <p><b>prefix-limit <i>number</i></b>—The number of prefixes that can be received from a peer router.</p> <p>The remaining statement is described separately.</p> |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring BGP Route Target Filtering for VPNs on page 38</a></li> <li>• <a href="#">Example: Configuring Proxy BGP Route Target Filtering</a></li> <li>• <a href="#">Example: Configuring an Export Policy for BGP Route Target Filtering for VPNs on page 66</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## graceful-restart (Enabling Globally)

---

|                            |                                                                                                                                                                                                                                                                                                    |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre>graceful-restart {   disable;   helper-disable;   maximum-helper-recovery-time <i>seconds</i>;   maximum-helper-restart-time <i>seconds</i>;   notify-duration <i>seconds</i>;   recovery-time <i>seconds</i>;   restart-duration <i>seconds</i>;   stale-routes-time <i>seconds</i>; }</pre> |
| <b>Hierarchy Level</b>     | [edit logical-systems <i>logical-system-name</i> routing-options],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> routing-options],<br>[edit routing-options],<br>[edit routing-instances <i>routing-instance-name</i> routing-options]        |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 12.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                         |
| <b>Description</b>         | Configure graceful restart globally to enable the feature. You cannot enable graceful restart for specific protocols unless graceful restart is also enabled globally. You can, optionally, modify the global settings at the individual protocol level.                                           |


**NOTE:**

- For VPNs, the **graceful-restart** statement allows a router whose VPN control plane is undergoing a restart to continue to forward traffic while recovering its state from neighboring routers.
  - For BGP, if you configure graceful restart after a BGP session has been established, the BGP session restarts and the peers negotiate graceful restart capabilities.
  - LDP sessions flap when **graceful-restart** configurations change.
- 

|                                 |                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>                  | Graceful restart is disabled by default.                                                                                                           |
| <b>Options</b>                  | The remaining statements are explained separately.                                                                                                 |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Enabling Graceful Restart</i></li><li>• <i>Configuring Routing Protocols Graceful Restart</i></li></ul> |

- *Configuring Graceful Restart for MPLS-Related Protocols*
- *Configuring VPN Graceful Restart*
- *Configuring Logical System Graceful Restart*
- *Graceful Restart Configuration Statements*
- *Configuring Graceful Restart for QFabric Systems*

## instance-type

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>instance-type type;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>     | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br><b>virtual-switch</b> and <b>layer2-control</b> options introduced in Junos OS Release 8.4.<br>Statement introduced in Junos OS Release 9.2 for EX Series switches.<br>Statement introduced in Junos OS Release 11.3 for the QFX Series.<br>Statement introduced in Junos OS Release 12.3 for ACX Series routers.<br><b>evpn</b> option introduced in Junos OS Release 13.2 for MX 3D Series routers.<br><b>forwarding</b> option introduced in Junos OS Release 14.2 for PTX Series Packet Transport Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>         | Define the type of routing instance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Options</b>             | <div>  <p><b>NOTE:</b> On ACX Series routers, you can configure only the forwarding, virtual router, and VRF routing instances.</p> </div> <p><b>type</b>—Can be one of the following:</p> <ul style="list-style-type: none"> <li><b>evpn</b>—(MX Series routers only) Enable an Ethernet VPN (EVPN) on the routing instance. You cannot configure the <b>evpn</b> option under the [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> instance-type] hierarchy level.</li> <li><b>forwarding</b>—Provide support for filter-based forwarding, where interfaces are not associated with instances. All interfaces belong to the default instance. Other instances are used for populating RPD learned routes. For this instance type, there is no one-to-one mapping between an interface and a routing instance. All interfaces belong to the default instance inet.0.</li> <li><b>l2backhaul-vpn</b>—Provide support for Layer 2 wholesale VLAN packets with no existing corresponding logical interface. When using this instance, the router learns both the outer tag and inner tag of the incoming packets, when the <b>instance-role</b> statement is defined as <b>access</b>, or the outer VLAN tag only, when the <b>instance-role</b> statement is defined as <b>nni</b>.</li> <li><b>l2vpn</b>—Enable a Layer 2 VPN on the routing instance. You must configure the <b>interface</b>, <b>route-distinguisher</b>, <b>vrf-import</b>, and <b>vrf-export</b> statements for this type of routing instance.</li> <li><b>layer2-control</b>—(MX Series routers only) Provide support for RSTP or MSTP in customer edge interfaces of a VPLS routing instance. This instance type cannot be used if the customer edge interface is multihomed to two provider edge interfaces. If the customer</li> </ul> |



edge interface is multihomed to two provider edge interfaces, use the default BPDU tunneling.

- **no-forwarding**—This is the default routing instance. Do not create a corresponding forwarding instance. Use this routing instance type when a separation of routing table information is required. There is no corresponding forwarding table. All routes are installed into the default forwarding table. IS-IS instances are strictly nonforwarding instance types.
- **virtual-router**—Enable a virtual router routing instance. This instance type is similar to a VPN routing and forwarding instance type, but used for non-VPN-related applications. You must configure the **interface** statement for this type of routing instance. You do not need to configure the **route-distinguisher**, **vrf-import**, and **vrf-export** statements.
- **virtual-switch**—(MX Series routers and EX9200 switches only) Provide support for Layer 2 bridging. Use this routing instance type to isolate a LAN segment with its Spanning Tree Protocol (STP) instance and to separate its VLAN identifier space.
- **vpls**—Enable VPLS on the routing instance. Use this routing instance type for point-to-multipoint LAN implementations between a set of sites in a VPN. You must configure the **interface**, **route-distinguisher**, **vrf-import**, and **vrf-export** statements for this type of routing instance.
- **vrf**—VPN routing and forwarding (VRF) instance. Provides support for Layer 3 VPNs, where interface routes for each instance go into the corresponding forwarding table only. Required to create a Layer 3 VPN. Create a VRF table (*instance-name.inet.0*) that contains the routes originating from and destined for a particular Layer 3 VPN. For this instance type, there is a one-to-one mapping between an interface and a routing instance. Each VRF instance corresponds with a forwarding table. Routes on an interface go into the corresponding forwarding table. You must configure the **interface**, **route-distinguisher**, **vrf-import**, and **vrf-export** statements for this type of routing instance.

**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

- Related Documentation**
- [Configuring the Instance Type on page 10](#)
  - [Configuring EVPN Routing Instances on page 239](#)
  - [Configuring EVPN Routing Instances on EX9200 Switches](#)
  - [Configuring Virtual Router Routing Instances](#)
  - [Example: Configuring Filter-Based Forwarding on the Source Address](#)
  - [Example: Configuring Filter-Based Forwarding on Logical Systems](#)
  - [Layer 2 Routing Instance Types](#)

## interface (Routing Instances)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>interface <i>interface-name</i> {<br/>    description <i>text</i>;<br/>}</code>                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> ]                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.2 for EX Series switches.<br>Statement introduced in Junos OS Release 12.3 for ACX Series routers.<br>Statement introduced in Junos OS Release 13.2 for MX 3D Series routers.                                                                          |
| <b>Description</b>              | Specify the interface over which the VPN traffic travels between the PE device and CE device. You configure the interface on the PE device. If the value <b>vrf</b> is specified for the <b>instance-type</b> statement included in the routing instance configuration, this statement is required.                                                    |
| <b>Options</b>                  | <i>interface-name</i> —Name of the interface.<br><br>The remaining statement is explained separately.                                                                                                                                                                                                                                                  |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Interfaces for VPN Routing on page 11</a></li><li>• <a href="#">Configuring EVPN Routing Instances on page 239</a></li><li>• <a href="#">Configuring EVPN Routing Instances on EX9200 Switches</a></li><li>• <a href="#">interface (VPLS Routing Instances) on page 1124</a></li></ul> |

## no-forwarding

---

|                                 |                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | no-forwarding;                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols ldp],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols ldp],<br>[edit protocols ldp],<br>[edit routing-instances <i>routing-instance-name</i> protocols ldp] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 12.3X50 for the QFX Series.                                                                                                                                                           |
| <b>Description</b>              | Do not add ingress routes to the inet.0 routing table even if <b>traffic-engineering bgp-igp</b> (configured at the [edit protocols mpls] hierarchy level) is enabled.                                                                                                              |
| <b>Default</b>                  | The <b>no-forwarding</b> statement is disabled. Ingress routes are added to the inet.0 routing table instead of the inet.3 routing table when <b>traffic-engineering bgp-igp</b> is enabled.                                                                                        |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Miscellaneous LDP Properties</a></li> <li>• <a href="#">Configuring a Routing Protocol Between the Service Provider Routers on page 15</a></li> </ul>                                                              |

## proxy-generate

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>proxy-generate &lt;route-target-policy <i>route-target-policy-name</i>&gt;;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | <code>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> family <i>route-target</i>],</code><br><code>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> family <i>route-target</i>],</code><br><code>[edit protocols bgp group <i>group-name</i> family <i>route-target</i>],</code><br><code>[edit protocols bgp group <i>group-name</i> neighbor <i>address</i> family <i>route-target</i>]</code>                                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Enable proxy BGP route target filtering (also known as proxy route target constrain, or proxy RTC). This feature is useful if you have a network environment where route target filtering is not widely deployed or fully supported. When configured for proxy BGP route target filtering, the device creates route target membership (RT membership) on behalf of its peers that do not have the route target filtering functionality. The device then distributes the RT membership advertisements from incoming BGP VPN routes to other devices in the network that need them. |
| <b>Options</b>                  | <code>route-target-policy <i>route-target-policy-name</i></code> —(Optional) Apply a routing policy that defines a subset of VPN routes to be used in your proxy BGP route target filter. The subset of VPN routes control which proxy BGP route targets are used to create the proxy BGP route target routes.                                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Example: Configuring Proxy BGP Route Target Filtering for VPNs on page 51</a></li><li>• <a href="#">Example: Configuring an Export Policy for BGP Route Target Filtering for VPNs on page 66</a></li><li>• <a href="#">Configuring BGP Route Target Filtering for VPNs on page 37</a></li><li>• <a href="#">family route-target on page 1041</a></li><li>• <a href="#">rtf-prefix-list on page 1055</a></li></ul>                                                                                                             |

## revert-time (Protocols Layer 2 Circuits)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>revert-time <i>seconds</i> maximum <i>seconds</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>     | <p>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i>],</p> <p>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i>]</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 10.2.</p> <p><b>maximum</b> option introduced in Junos OS Release 13.2.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>         | <p>Specify a revert time for redundant Layer 2 circuits and VPLS pseudowires. When you have configured redundant pseudowires for Layer 2 circuits or VPLS, traffic is switched to the backup connection in the event that the primary connection fails. If you configure a revert time, when the configured time expires traffic is reverted to the primary path, assuming the primary path has been restored.</p> <p>With the <b>maximum</b> option, specify a maximum reversion interval to add after the <b>revert-time</b> delay. If a revert-time delay is defined but a maximum timer is not defined, VCs are restored upon the revert-timer's expiration.</p> <p>To reduce as much as possible the amount of traffic discarded, and potential data-path asymmetries observed during primary-to-backup transition periods, you can use this restoration timer. This restoration timer is activated when the backup path is performing as active, and then the primary path is restored. The goal is to avoid moving traffic back to the primary path right away, to make sure that the control plane's related tasks (such as IGP, LDP, RSVP, and internal BGP) have enough time to complete their updating cycle.</p> <p>By enabling a gradual return of traffic to the primary path, you can ensure that the relatively-slow control-plane processing and updating does not have a negative impact on the restoration process.</p> <p>The <b>maximum</b> option extends the revert timer's functionality to provide a jittered interval over which a certain number of circuits can be transitioned back to the primary path. By making use of this maximum value, you can define a time interval during which circuits are expected to switch over. As a consequence, circuits' effective transitions are scattered during restoration periods.</p> <p>When making use of <b>revert-time x maximum y</b> statement, you can ensure that the corresponding circuit that is active is moved to the primary path within a time-slot (t1) such as that: <math>x \leq t1 \leq y</math>. In other words, by activating this statement, you can ensure the following:</p> <ul style="list-style-type: none"> <li>• VCs stay in the backup path for at least x seconds after the primary path comes back up.</li> <li>• VCs are moved back to the primary path before y seconds have elapsed.</li> <li>• y maximum value = x maximum value * 2 = 1200 seconds.</li> </ul> |

The ideal values for x and y will be conditioned to internal aspects of your network. For this reason, there are no default values for these settings. If no `revert-time` is set, the default behavior is non-revertive. That is, circuits are not returned to the primary path upon restoration. They are kept on the backup path.

**Default** Without the **`revert-time`** statement, virtual circuit (VC) traffic is not transitioned to the primary path upon restoration of the primary path.

**Options** *seconds*—Revert time in seconds.

**Range:** 0 through 600 seconds

*maximum seconds*—Number of seconds to delay path restoration after the **`revert-time`** delay.

**Range:** 0 through 1200 seconds

**Required Privilege** routing—To view this statement in the configuration.

**Level** routing-control—To add this statement to the configuration.

**Related Documentation** • [Configuring Redundant Pseudowires for Layer 2 Circuits and VPLS on page 179](#)

## route-distinguisher

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>route-distinguisher (as-number:id   ip-address:id);</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>     | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn mesh-group <i>mesh-group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn mesh-group <i>mesh-group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>]</p>                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b> | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 11.1 for EX Series switches.</p> <p>Support at [edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>] hierarchy level introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3 for ACX Series routers.</p> <p>Support at [edit routing-instances <i>routing-instance-name</i> protocols l2vpn mesh-group <i>mesh-group-name</i>] hierarchy level introduced in Junos OS Release 13.2.</p> <p>Statement introduced in Junos OS Release 14.1X53-D30 for QFX Series switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>         | <p>Specify an identifier attached to a route, enabling you to distinguish to which VPN or virtual private LAN service (VPLS) the route belongs. Each routing instance must have a unique route distinguisher (RD) associated with it. The RD is used to place bounds around a VPN so that the same IP address prefixes can be used in different VPNs without having them overlap. If the instance type is <b>vrf</b>, the <b>route-distinguisher</b> statement is required.</p> <p>For Layer 2 VPNs and VPLS, if you configure the <b>l2vpn-use-bgp-rules</b> statement, you must configure a unique RD for each PE router participating in the routing instance.</p> <p>For other types of VPNs, we recommend that you use a unique RD for each provider edge (PE) router participating in specific routing instance. Although you can use the same RD on all PE routers for the same VPN routing instance, if you use a unique RD, you can determine the customer edge (CE) router from which a route originated within the VPN.</p> <p>For Layer 2 VPNs and VPLSs, if you configure mesh groups, the RD in each mesh group must be unique.</p> |



**CAUTION:** We strongly recommend that if you change an RD that has already been configured, make the change during a maintenance window, as follows:

1. Deactivate the routing instance.
2. Change the RD.
3. Activate the routing instance.

This is not required if you are configuring the RD for the first time.

**Options** *as-number: number*—*as-number* is an assigned AS number, and *number* is any 2-byte or 4-byte value. The AS number can be from 1 through 4,294,967,295. If the AS number is a 2-byte value, the administrative number is a 4-byte value. If the AS number is a 4-byte value, the administrative number is a 2-byte value. An RD consisting of a 4-byte AS number and a 2-byte administrative number is defined as a type 2 RD in RFC 4364 *BGP/MPLS IP VPNs*.



**NOTE:** In Junos OS Release 9.1 and later, the numeric range for AS numbers is extended to provide BGP support for 4-byte AS numbers, as defined in RFC 4893, *BGP Support for Four-octet AS Number Space*. All releases of Junos OS support 2-byte AS numbers. To configure an RD that includes a 4-byte AS number, append the letter “L” to the end of the AS number. For example, an RD with the 4-byte AS number 7,765,000 and an administrative number of 1,000 is represented as 7765000L:1000.

In Junos OS Release 9.2 and later, you can also configure a 4-byte AS number using the AS dot notation format of two integer values joined by a period: *<16-bit high-order value in decimal>.<16-bit low-order value in decimal>*. For example, the 4-byte AS number of 65,546 in the plain-number format is represented as 1.10 in AS dot notation format.

*ip-address: id*—IP address (*ip-address* is a 4-byte value) within your assigned prefix range and a 2-byte value for the *id*. The IP address can be any globally unique unicast address.

**Range:** 0 through 4,294,967,295 ( $2^{32} - 1$ ). If the router you are configuring is a BGP peer of a router that does not support 4-byte AS numbers, you need to configure a local AS number. For more information, see *Using 4-Byte Autonomous System Numbers in BGP Networks Technology Overview*.


**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**

- [Example: Configuring BGP Route Target Filtering for VPNs on page 41](#)
- [Example: Configuring FEC 129 BGP Autodiscovery for VPWS on page 708](#)
- [Configuring EVPN Routing Instances on page 239](#)
- [Configuring the Route Distinguisher on page 13](#)
- [Configuring an MPLS-Based Layer 2 VPN \(CLI Procedure\)](#)
- [Configuring an MPLS-Based Layer 3 VPN \(CLI Procedure\)](#)
- [l2vpn-use-bgp-rules on page 1133](#)



## route-distinguisher-id

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>route-distinguisher-id <i>ip-address</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-options],<br>[edit routing-options]                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | <p>Automatically assign a route distinguisher to the routing instance.</p> <p>If you configure the <b>route-distinguisher</b> statement in addition to the <b>route-distinguisher-id</b> statement, the value configured for <b>route-distinguisher</b> supersedes the value generated from <b>route-distinguisher-id</b>.</p>                                                                                                                             |
|                                 | <div>  <p><b>NOTE:</b> To avoid a conflict in the two route distinguisher values, it is recommended to ensure that the first half of the route distinguisher obtained by configuring the <b>route-distinguisher</b> statement is different from the first half of the route distinguisher obtained by configuring the <b>route-distinguisher-id</b> statement.</p> </div> |
| <b>Options</b>                  | <i>ip-address</i> —Address for routing instance.                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring BGP Route Target Filtering for VPNs on page 41</a></li> <li>• <a href="#">Configuring the Route Distinguisher on page 13</a></li> </ul>                                                                                                                                                                                                                                          |

## route-target-filter

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>route-target-filter <i>destination</i> {<br/>    group <i>group-name</i>;<br/>    local;<br/>    neighbor <i>address</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-options rib bgp.rtarget.0 static],<br>[edit routing-options rib bgp.rtarget.0 static]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.2.<br>Statement introduced in Junos OS Release 12.3 for ACX Series routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | Statically configure route target filtering. Route target filtering allows you to distribute VPN routes to only the routers that need them. In VPN networks without route target filtering configured, BGP distributes all static VPN routes to all of the VPN peer routers. You can add static routes to the bgp.rtarget.0 routing table with specific NLRI-imposed constraints.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>                  | <p><b><i>destination</i></b>—Allows you to specify the static route destination. This value must be in the format x:y/len. 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, 123456L:100/64).</p> <p><b><i>group group-name(s)</i></b>—Installs an RT-Constrain filter for the destination for all peers in the specified BGP group. The route and corresponding BGP group are displayed in the output of the <b>show bgp group rtf detail</b> command.</p> <p><b><i>local</i></b>—Causes the router to originate the route target constrain NLRI, but does not install any filtering state for the prefix. This behavior can be useful when the router should always receive VPN routes with this route-target regardless of the state of a given BGP peering session or group status. The route is not displayed in the output of the <b>show bgp group rtf detail</b> command unless it is also included in either the BGP neighbor or BGP group configuration.</p> <p><b><i>neighbor address</i></b>—Installs an RT-Constrain filter for the destination for this BGP neighbor. The route is displayed in the output of the <b>show bgp group rtf detail</b> command. Specify the BGP neighbor using the router's IP address.</p> |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Static Route Target Filtering for VPNs on page 49</a></li><li>• <a href="#">Reducing Network Resource Use with Static Route Target Filtering for VPNs on page 82</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## rtf-prefix-list

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>rtf-prefix-list <i>name</i> route-targets</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | <p>[edit logical-systems <i>logical-system-name</i> policy-options],</p> <p>[edit logical-systems <i>logical-system-name</i> policy-options policy-statement <i>policy-name</i> term <i>term-name</i>],</p> <p>[edit policy-options],</p> <p>[edit policy-options policy-statement <i>policy-name</i> term <i>term-name</i>]</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | <p>Define a list of route target prefixes for use in a routing policy statement. These prefixes are only useful for filtering routes in the <code>bgp.target.0</code> table.</p> <p>The route target filtering prefix is in the format: <i>AS number:route target extended community/length</i>. The first number represents the autonomous system (AS) of the device that sent the advertisement. The second group of numbers represent the route target extended community. The format of the extended community is the same as the extended community type <b>target</b>. For more information about extended communities, see <i>Understanding How to Define BGP Communities and Extended Communities</i>.</p> <p>In this route target prefix example <code>64500:200:101/96</code>, <code>64500</code> is the AS number, <code>200:101</code> is the BGP extended community used for the route target, and <code>96</code> is the prefix length.</p> <p>For more information about the route target community, see RFC 4360, <i>BGP Extended Communities Attribute</i>.</p> <p>For more information about the route target filtering prefix format, see RFC 4684, <i>Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)</i>.</p> |
| <b>Options</b>                  | <p><b><i>name</i></b>—Name that identifies the list of route target filtering prefixes. The name can contain letters, numbers, and hyphens ( - ) and can be up to 255 characters long. To include spaces in the name, enclose the entire name in quotation marks ( " ").</p> <p><b><i>route-targets</i></b>—List of route target filtering prefixes, one route target filter per line in the configuration. When you use the <b>rtf-prefix-list</b> statement as a match condition, you do not have the option of configuring the list of route target filtering prefixes. You must first define and configure the route target filtering prefixes with the <b>policy-options</b> statement.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring an Export Policy for BGP Route Target Filtering for VPNs on page 66</a></li> <li>• <a href="#">Configuring BGP Route Target Filtering for VPNs on page 37</a></li> <li>• <a href="#">Understanding Proxy BGP Route Target Filtering for VPNs on page 50</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

- [Understanding How to Define BGP Communities and Extended Communities](#) in the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*
- [family route-target](#) on page 1041

---

## switchover-delay

---

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                   | switchover-delay <i>milliseconds</i> ;                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Hierarchy Level          | [edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i> ],<br>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i> ] |
| Release Information      | Statement introduced in Junos OS Release 9.2.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Description              | After the primary pseudowire goes down, specifies the delay (in milliseconds) to wait before the backup pseudowire takes over. You configure this statement for each backup neighbor configuration to adjust the switchover time after a failure is detected.                                                                                                                                                                                                         |
| Options                  | <b>milliseconds</b> —Specify the time to wait before switching to the backup pseudowire after the primary pseudowire fails.<br><b>Default:</b> 10,000 milliseconds<br><b>Range:</b> 0 through 180,000 milliseconds                                                                                                                                                                                                                                                    |
| Required Privilege Level | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                   |
| Related Documentation    | • <a href="#">Configuring the Switchover Delay for the Pseudowires</a> on page 180                                                                                                                                                                                                                                                                                                                                                                                    |

## unicast-reverse-path

|                                 |                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | unicast-reverse-path (active-paths   feasible-paths);                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-options forwarding-table],<br>[edit routing-instances <i>routing-instance-name</i> instance-type <i>name</i> routing-options forwarding-table],<br>[edit routing-options forwarding-table]                                                                                          |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Support for routing instances added in Junos OS Release 8.3.<br>Statement introduced in Junos OS Release 12.3 for ACX Series routers.                                                                                                                                                   |
| <b>Description</b>              | Control the operation of unicast reverse-path-forwarding check. This statement enables the RPF check to be used when routing is asymmetrical.                                                                                                                                                                                                |
| <b>Options</b>                  | <p><b>active-paths</b>—Consider only active paths during the unicast reverse-path check.</p> <p><b>feasible-paths</b>—Consider all feasible paths during the unicast reverse-path check.</p> <p><b>Default:</b> If you omit the <b>unicast-reverse-path</b> statement, only the active paths to a particular destination are considered.</p> |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring Unicast Reverse-Path-Forwarding Check on page 103</a></li> <li>• <a href="#">Enabling Unicast Reverse-Path Forwarding Check for VPNs on page 102</a></li> </ul>                                                                                                    |

## vpn-apply-export

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | vpn-apply-export;                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols bgp],<br>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> neighbor<br><i>neighbor</i> ],<br>[edit protocols bgp],<br>[edit protocols bgp group <i>group-name</i> ],<br>[edit protocols bgp group <i>group-name</i> neighbor <i>neighbor</i> ] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | Apply both the VRF export and BGP group or neighbor export policies (VRF first, then BGP) before routes from the <b>vrf</b> or <b>l2vpn</b> routing tables are advertised to other PE routers.                                                                                                                                                                                                                                              |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Applying Both the VRF Export and the BGP Export Policies on page 30</a></li></ul>                                                                                                                                                                                                                                                                                                       |

## vrf-export

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>vrf-export [ <i>policy-names</i> ];</code>                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>],<br/> [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols<br/> vpls mesh-group <i>mesh-group-name</i>]<br/> [edit routing-instances <i>routing-instance-name</i>]<br/> [edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>]<br/> [edit switch-options]</p> |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 11.1 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 12.3 for ACX Series routers.</p> <p>Statement introduced in Junos OS Release 14.1X53-D30 for QFX Series switches.</p>                                                                                                                                                                |
| <b>Description</b>              | <p>Specify how routes are exported from the local PE router's VRF table (<i>routing-instance-name</i>.inet.0) to the remote PE router. If the value <b>vrf</b> is specified for the <b>instance-type</b> statement included in the routing instance configuration, this statement is required.</p> <p>You can configure multiple export policies on the PE router or PE switch.</p>                                                                                    |
| <b>Default</b>                  | If the instance-type is <b>vrf</b> , <b>vrf-export</b> is a required statement. The default action is to reject.                                                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>                  | <i>policy-names</i> —Names for the export policies.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Implementing EVPN-VXLAN for Data Centers</i></li> <li>• <a href="#">instance-type on page 1044</a></li> <li>• <a href="#">Configuring an Export Policy for the PE Router's VRF Table on page 29</a></li> </ul>                                                                                                                                                                                                             |

## vrf-import

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>vrf-import [ <i>policy-names</i> ];</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>],</code><br><code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols</code><br><code>    vpls mesh-group <i>mesh-group-name</i>]</code><br><code>[edit routing-instances <i>routing-instance-name</i>]</code><br><code>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>]</code><br><code>[edit switch-options]</code> |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 11.1 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D30 for QFX Series switches.                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | <p>Specify how routes are imported into the virtual routing and forwarding (VRF) table (<i>routing-instance-name</i>.inet.0) of the local provider edge (PE) router or switch from the remote PE router. If the value <b>vrf</b> is specified for the <b>instance-type</b> statement included in the routing instance configuration, this statement is required.</p> <p>You can configure multiple import policies on the PE router or switch.</p>                                                                                      |
| <b>Default</b>                  | If the instance type is <b>vrf</b> , <b>vrf-import</b> is a required statement. The default action is to accept.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <i>policy-names</i> —Names for the import policies.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Implementing EVPN-VXLAN for Data Centers</i></li><li>• <a href="#">instance-type on page 1044</a></li><li>• <a href="#">Configuring an Import Policy for the PE Router's VRF Table on page 27</a></li></ul>                                                                                                                                                                                                                                                                                  |



---

## vrf-mtu-check

---

|                                 |                                                                                                                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | vrf-mtu-check;                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit chassis]                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 11.1 for EX Series switches.                                                                                                                                                                    |
| <b>Description</b>              | On M Series routers (except the M120 and M320 router), T Series routers, and on EX Series 8200 switches, configure path maximum transmission unit (MTU) checks on the outgoing interface for unicast traffic routed on a virtual private network (VPN) routing and forwarding (VRF) instance. |
| <b>Default</b>                  | Disabled.                                                                                                                                                                                                                                                                                     |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Path MTU Checks for VPN Routing Instances on page 16</a></li><li>• <i>Configuring the Junos OS to Enable MTU Path Check for a Routing Instance on M Series Routers</i></li></ul>                                              |

## vrf-target

---

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                   | <pre>vrf-target {<br/>    community;<br/>    auto<br/>    import community-name;<br/>    export community-name;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Hierarchy Level          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn mesh-group <i>mesh-group-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn mesh-group <i>mesh-group-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> ],<br>[edit switch-options]                  |
| Release Information      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 11.1 for EX Series switches.<br>Statement introduced in Junos OS Release 12.3 for ACX Series routers.<br>Statement introduced in Junos OS Release 14.1X53-D30 for QFX Series switches. <b>auto option</b> was also added at this time.                                                                                                                                                                                                                                                                                                                                                                                                            |
| Description              | <p>Specify a virtual routing and forwarding (VRF) target community. If you configure the <b>community</b> option only, default VRF import and export policies are generated that accept and tag routes with the specified target community. The purpose of the <b>vrf-target</b> statement is to simplify the configuration by allowing you to configure most statements at the [edit routing-instances] hierarchy level. In effect, this statement configures a single policy for import and a single policy for export to replace the per-VRF policies for every community.</p> <p>You can still create more complex policies by explicitly configuring VRF import and export policies using the <b>import</b> and <b>export</b> options.</p> |
| Options                  | <p><b>community</b>—Community name.</p> <p><b>auto</b>—Automatically derives the route target (RT) for supported QFX Series switches.</p> <p><b>import community-name</b>—Allowed communities accepted from neighbors.</p> <p><b>export community-name</b>—Allowed communities sent to neighbors.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Required Privilege Level | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Related Documentation    | <ul style="list-style-type: none"><li>• <i>Implementing EVPN-VXLAN for Data Centers</i></li><li>• <a href="#">Configuring a VRF Target on page 31</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

- [Example: Configuring FEC 129 BGP Autodiscovery for VPWS on page 708](#)



# Configuration Statements (Layer 2 VPNs and VPLS)

- [action-priority](#) on page 1069
- [active-interface](#) (VPLS Multihoming) on page 1070
- [any](#) (VPLS Multihoming) on page 1071
- [auto-discovery-only](#) on page 1072
- [automatic-site-id](#) on page 1073
- [backup-interface](#) (Layer 2 Circuits) on page 1074
- [bandwidth](#) (Protocols Layer 2 Circuit) on page 1075
- [best-site](#) on page 1076
- [bfd-liveness-detection](#) (Layer 2 VPN and VPLS) on page 1077
- [community](#) (Protocols Layer 2 Circuit) on page 1078
- [connection-protection](#) on page 1079
- [connectivity-type](#) on page 1080
- [control-channel](#) (Protocols OAM) on page 1081
- [control-word](#) (Protocols Layer 2 Circuit Neighbor) on page 1082
- [control-word](#) (Protocols Layer 2 VPN) on page 1083
- [control-word](#) (BGP VPLS) on page 1084
- [description](#) (Protocols Layer 2 Circuit Neighbor) on page 1084
- [description](#) (Protocols Layer 2 VPN) on page 1085
- [detection-time](#) (BFD Liveness Detection) on page 1086
- [encapsulation](#) (Logical Interface) on page 1088
- [encapsulation](#) (Physical Interface) on page 1092
- [encapsulation-type](#) (Layer 2 Circuits) on page 1097
- [encapsulation-type](#) (Layer 2 VPNs) on page 1099
- [egress-protection](#) (Layer 2 circuit) on page 1100
- [egress-protection](#) (MPLS) on page 1101
- [end-interface](#) on page 1102

- [esi](#) on page 1103
- [extended-vlan-list](#) on page 1104
- [family](#) on page 1105
- [family multiservice](#) on page 1109
- [fast-aps-switch](#) on page 1111
- [fast-reroute-priority](#) on page 1112
- [flow-label-receive-static](#) on page 1113
- [flow-label-transmit-static](#) on page 1113
- [hot-standby](#) on page 1114
- [hot-standby \(Protocols Layer 2 Circuit\)](#) on page 1115
- [hot-standby-vc-on \(Protocols Layer 2 Circuit\)](#) on page 1116
- [identifier \(VPLS Multihoming for FEC 129\)](#) on page 1117
- [ignore-encapsulation-mismatch](#) on page 1118
- [ignore-mtu-mismatch](#) on page 1119
- [interface \(EVPN Routing Instances\)](#) on page 1120
- [interface \(Protocols Layer 2 Circuit\)](#) on page 1121
- [interface \(Protocols Layer 2 VPN\)](#) on page 1122
- [interface \(VPLS Multihoming for FEC 129\)](#) on page 1123
- [interface \(VPLS Routing Instances\)](#) on page 1124
- [interface-mac-limit \(VPLS\)](#) on page 1125
- [install-nexthop](#) on page 1126
- [l2circuit](#) on page 1127
- [l2ckt](#) on page 1128
- [l2vpn](#) on page 1129
- [l2vpn \(routing-options\)](#) on page 1131
- [l2vpn-id](#) on page 1132
- [l2vpn-use-bgp-rules](#) on page 1133
- [label-allocation](#) on page 1133
- [label-block-size](#) on page 1134
- [label-switched-path-template \(Multicast\)](#) on page 1135
- [local-switching \(Layer 2 Circuits\)](#) on page 1136
- [local-switching \(VPLS\)](#) on page 1137
- [mac-flush](#) on page 1138
- [mac-statistics](#) on page 1140
- [mac-table-aging-time](#) on page 1142
- [mac-table-size](#) on page 1143
- [mesh-group \(Protocols VPLS\)](#) on page 1144

- [minimum-interval \(BFD Liveness Detection\)](#) on page 1146
- [minimum-interval \(transmit-interval\)](#) on page 1148
- [minimum-receive-interval \(BFD Liveness Detection\)](#) on page 1150
- [mtu](#) on page 1152
- [multiplier \(BFD Liveness Detection\)](#) on page 1156
- [multi-homing \(VPLS Multihoming for FEC 128\)](#) on page 1157
- [multi-homing \(VPLS Multihoming for FEC 129\)](#) on page 1158
- [neighbor \(Protocols Layer 2 Circuit\)](#) on page 1159
- [neighbor \(Protocols VPLS\)](#) on page 1161
- [no-adaptation \(BFD Liveness Detection\)](#) on page 1163
- [no-control-word \(BGP VPLS\)](#) on page 1164
- [no-control-word \(Protocols Layer 2 VPN\)](#) on page 1165
- [no-l2ckt](#) on page 1166
- [no-l2vpn](#) on page 1166
- [no-local-switching \(VPLS\)](#) on page 1167
- [no-mac-learning](#) on page 1168
- [no-revert \(Local Switching\)](#) on page 1170
- [no-revert \(Neighbor Interface\)](#) on page 1171
- [no-tunnel-services](#) on page 1172
- [oam](#) on page 1173
- [packet-action](#) on page 1174
- [peer-active \(VPLS Multihoming for FEC 129\)](#) on page 1177
- [peer-as \(VPLS\)](#) on page 1178
- [ping-interval](#) on page 1179
- [policer \(Layer 2 VPN\)](#) on page 1180
- [preference \(Interface-Level Preference for VPLS Multihoming for FEC 129\)](#) on page 1181
- [preference \(Site-Level Preference for VPLS Multihoming for FEC 129\)](#) on page 1182
- [primary \(VPLS Multihoming\)](#) on page 1183
- [protect-interface](#) on page 1184
- [protected-l2circuit](#) on page 1185
- [protector-interface](#) on page 1186
- [protector-pe](#) on page 1186
- [proxy \(Interfaces\)](#) on page 1187
- [pseudowire-status-tlv](#) on page 1187
- [psn-tunnel-endpoint](#) on page 1188
- [remote](#) on page 1189
- [remote-site-id](#) on page 1189

- [routing-instances](#) on page 1190
- [rsvp-te \(Routing Instances Provider Tunnel\)](#) on page 1191
- [send-oam](#) on page 1191
- [site \(Layer 2 Circuits\)](#) on page 1192
- [site \(VPLS Multihoming for FEC 128\)](#) on page 1193
- [site \(VPLS Multihoming for FEC 129\)](#) on page 1194
- [site-identifier \(Layer 2 Circuits\)](#) on page 1195
- [site-identifier \(VPLS\)](#) on page 1195
- [site-preference](#) on page 1196
- [site-range](#) on page 1197
- [source-attachment-identifier \(Protocols VPWS\)](#) on page 1198
- [standby \(Protocols Layer 2 Circuit\)](#) on page 1199
- [static \(Protocols Layer 2 Circuit\)](#) on page 1200
- [static \(Protocols VPLS\)](#) on page 1201
- [static-mac](#) on page 1202
- [target-attachment-identifier \(Protocols VPWS\)](#) on page 1203
- [template](#) on page 1204
- [threshold \(detection-time\)](#) on page 1205
- [threshold \(transmit-interval\)](#) on page 1207
- [traceoptions \(Egress Protection\)](#) on page 1209
- [traceoptions \(Protocols EVPN\)](#) on page 1210
- [traceoptions \(Protocols Layer 2 Circuit\)](#) on page 1212
- [traceoptions \(Protocols Layer 2 VPN\)](#) on page 1214
- [traceoptions \(Protocols VPLS\)](#) on page 1216
- [transmit-interval \(BFD Liveness Detection\)](#) on page 1218
- [tunnel-services \(Routing Instances VPLS\)](#) on page 1220
- [version \(BFD Liveness Detection\)](#) on page 1221
- [virtual-circuit-id](#) on page 1222
- [virtual-mac](#) on page 1223
- [vlan-id](#) on page 1223
- [vlan-id \(routing instance\)](#) on page 1224
- [vlan-id-list \(Interface in VPLS\)](#) on page 1225
- [vlan-tagging](#) on page 1226
- [vpls \(Interfaces\)](#) on page 1226
- [vpls \(Routing Instance\)](#) on page 1227
- [vpls-id](#) on page 1229




- [vpls-id-list \(protocols vpls mesh-group\) on page 1230](#)
- [vpls-mac-move on page 1231](#)

## action-priority


|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>action-priority value;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit routing-instances <i>routing-instance-name</i> protocols <i>protocol-name</i> interface <i>interface-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | <p>Configure the priority for an interface on which the MAC move action will be applied. When a MAC move is configured with a corresponding action, and that limit is exceeded, the action is applied to one of the interfaces associated with that MAC address having the highest action priority. If the action configured for the MAC move is <b>shutdown</b>, you can use the action priority to determine which interface is disabled. If an interface is trusted, assign a low action priority to decrease the likelihood that the interface will be shutdown if the configured action is <b>shutdown</b> or <b>vlan-member-shutdown</b>.</p> <p>If no action priority is configured, or if the interfaces have the same action priority, then the action is applied to the interface to which the MAC address moved last.</p>                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <p><b>value</b>—Value assigned to an interface associated with a MAC address move. The value determines the priority with which an action is applied to the interface if the MAC address move limit is reached. The interface with the highest priority is the interface with the lowest value configured for <b>action-priority</b>.</p> <p>A higher value means lower priority. For example, if a MAC address move occurs between two interfaces with the action priority value set to 5 and 6, the interface with value 5 as the action priority value is blocked.</p> <p>If a VPLS instance has MAC move action enabled, set the <b>action-priority</b> to 8 for the router to detect an interface as a core interface by the VPLS customer edge loop prevention feature. By default, the loop prevention feature supports <b>lsi</b> and <b>vt</b>-type interfaces as core interfaces, however, you can use this special action-priority value to designate any interface as a core interface.</p> <p><b>Default:</b> The default value is 4.</p> <p><b>Range:</b> 0 through 8</p> |
| <b>Required Privilege Level</b> | <p>system—To view this statement in the configuration.</p> <p>system—control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">MAC Moves Loop Prevention in VPLS Network Overview on page 900</a></li> <li>• <a href="#">Example: Configuring Loop Prevention in VPLS Network Due to MAC Moves on page 904</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## active-interface (VPLS Multihoming)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>active-interface {<br/>    any;<br/>    primary interface-name;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | <pre>[edit logical-systems logical-system-name routing-instances instance-name protocols vpls multi-homing],<br/>[edit logical-systems logical-system-name routing-instances instance-name protocols vpls multi-homing site site-name],<br/>[edit routing-instances instance-name protocols vpls multi-homing],<br/>[edit routing-instances instance-name protocols vpls multi-homing site site-name]</pre>                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | <p>Specify a multihomed interface as the primary interface for the VPLS site. If there are multiple interfaces, the remaining interfaces are activated only when the primary interface goes down. If no active interfaces are configured at the site level, it is assumed that all traffic for a VPLS site travels through a single, nonmultihomed PE router.</p> <div> <b>NOTE:</b> In the VPLS documentation, the word <i>router</i> in terms such as <i>PE router</i> is used to refer to any device that provides routing functions.</div> <p>The remaining statements are explained separately.</p> <p>For FEC 128, use the <code>[edit routing-instances instance-name protocols vpls multi-homing]</code> hierarchy level.</p> |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Specifying an Interface as the Active Interface on page 754</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## any (VPLS Multihoming)

|                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                          | any;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                 | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls multi-homing active-interface],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls multi-homing site <i>site-name</i> active-interface],</p> <p>[edit routing-instances <i>instance-name</i> protocols vpls multi-homing active-interface],</p> <p>[edit routing-instances <i>instance-name</i> protocols vpls multi-homing site <i>site-name</i> active-interface]</p> |
| <b>Release Information</b>                                                                                                                                                                                                                                             | Statement introduced in Junos OS Release 7.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>                                                                                                                                                                                                                                                     | Specify that any multihomed interface can be used as the primary interface by the VPLS site. Depending on the order in which interfaces are listed in the PE router's configuration, the first operational interface in the set of configured interfaces is chosen to be the primary interface.                                                                                                                                                                                                                                              |
| <div>  <p><b>NOTE:</b> In the VPLS documentation, the word <i>router</i> in terms such as <i>PE router</i> is used to refer to any device that provides routing functions.</p> </div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| For FEC 128, use the [edit routing-instances <i>instance-name</i> protocols vpls multi-homing active-interface] hierarchy level.                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Default</b>                                                                                                                                                                                                                                                         | This is the default behavior.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                        | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>                                                                                                                                                                                                                                           | <ul style="list-style-type: none"> <li>• <a href="#">Specifying an Interface as the Active Interface on page 754</a></li> <li>• <a href="#">primary on page 1183</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                              |

## auto-discovery-only

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | auto-discovery-only;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>          | <p>[edit logical-systems <i>logical-system-name</i> protocols bgp family l2vpn],<br/>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> family l2vpn],<br/>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> family l2vpn],<br/>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols bgp family l2vpn],<br/>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols bgp group <i>group-name</i> family l2vpn],<br/>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> family l2vpn],<br/>[edit protocols bgp family l2vpn],<br/>[edit protocols bgp group <i>group-name</i> family l2vpn],<br/>[edit protocols bgp group <i>group-name</i> neighbor <i>address</i> family l2vpn],<br/>[edit routing-instances <i>instance-name</i> protocols bgp family l2vpn],<br/>[edit routing-instances <i>instance-name</i> protocols bgp group <i>group-name</i> family l2vpn],<br/>[edit routing-instances <i>instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> family l2vpn]</p> |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.4R2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | <p>Enable the router to process only the autodiscovery network layer reachability information (NLRI) update messages for VPWS and LDP-based Layer 2 VPN and VPLS update messages (BGP_L2VPN_AD_NLRI) (FEC 129).</p> <p>Specifically, the <b>auto-discovery-only</b> statement notifies the routing process (rpd) to expect autodiscovery-related NLRI messages so that information can be deciphered and used by LDP, VPLS, and VPWS.</p> <p>The <b>auto-discovery-only</b> statement must be configured on all provider edge (PE) routers in a VPLS or in a VPWS. If you configure route reflection, the <b>auto-discovery-only</b> statement is also required on provider (P) routers that act as the route reflector in supporting FEC 129-related updates.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Example: Configuring BGP Autodiscovery for LDP VPLS on page 725</a></li><li>• <a href="#">Example: Configuring BGP Autodiscovery for LDP VPLS with User-Defined Mesh Groups on page 742</a></li><li>• <a href="#">Example: Configuring FEC 129 BGP Autodiscovery for VPWS on page 708</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## automatic-site-id

|                            |                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre>automatic-site-id {   collision-detect-time <i>seconds</i>;   new-site-wait-time <i>seconds</i>;   reclaim-wait-time minimum <i>seconds</i> maximum <i>seconds</i>;   startup-wait-time <i>seconds</i>; }</pre>                                                                                                                                                                    |
| <b>Hierarchy Level</b>     | <pre>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i>]</pre>                                                                                                                                            |
| <b>Release Information</b> | Statement introduced in Junos OS Release 9.1.                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>         | <p>Enable automatic site identifiers for VPLS routing instances.</p> <p>When you configure <b>automatic-site-id</b> for the first time, you must deactivate and then activate <b>protocol vpls</b>. However, if you already have <b>automatic-site-id</b> configured, you do not need to deactivate and then activate <b>protocol vpls</b>.</p>                                         |
| <b>Options</b>             | <p><b>collision-detect-time</b>—The time in seconds to wait after a claim advertisement is sent to the other routers in a VPLS instance before a PE router can begin using a site identifier. If the PE router receives a competing claim advertisement for the same site identifier during this time period, it initiates the collision resolution procedure for site identifiers.</p> |



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

**new-site-wait-time**—The time in seconds to wait to receive VPLS information for a newly configured routing instance or a new site. This time interval is also applied whenever the automatic site identifier feature is activated on a VPLS routing instance other than at startup. Effectively, this timer indicates how long to wait before an attempt is made to allocate a site identifier. This timer is also triggered whenever a VPLS routing instance is enabled.

**reclaim-wait-time**—The time in seconds to wait to receive VPLS information for a newly configured routing instance or a new site. This time interval is also applied whenever the automatic site identifier feature is activated on a VPLS routing instance other than at startup. Effectively, this timer indicates how long to wait before an attempt is made to allocate a site identifier. This timer is also triggered whenever a VPLS routing instance is enabled. You can configure two values for this option: the **minimum** wait time and the **maximum** wait time.

**startup-wait-time**—The time in seconds to wait at startup to receive all the VPLS information for the route targets configured on the other PE routers included in the VPLS routing instance.

**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Automatic Site Identifiers for VPLS on page 566](#)

---

## backup-interface (Layer 2 Circuits)

---

**Syntax** backup-interface *interface-name*;

**Hierarchy Level** [edit logical-systems *logical-system-name* protocols l2circuit local-switching interface *interface-name* end-interface interface *interface-name*],  
[edit protocols l2circuit local-switching interface *interface-name* end-interface interface *interface-name*]

**Release Information** Statement introduced in Junos OS Release 12.3.

**Description** Specify the interface to be used by the protection pseduowire in connection protection configurations for Layer 2 circuits.

**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration

**Related Documentation**


- [Example: Configuring Layer 2 Circuit Switching Protection on page 420](#)

## bandwidth (Protocols Layer 2 Circuit)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>bandwidth (<i>bandwidth</i>   <i>ctnumber bandwidth</i>);</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> ],<br>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> ]                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>              | Specify bandwidth allocation for a Layer 2 circuit or for the class types of a Layer 2 circuit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Options</b>                  | <p><b><i>bandwidth</i></b>—Configure the bandwidth in bits per second for the Layer 2 circuit. You cannot configure the bandwidth for the Layer 2 circuit and for the class types at the same time.</p> <p><b><i>ctnumber bandwidth</i></b>—Configure the bandwidth in bits per second for a class type on the Layer 2 circuit. You can configure bandwidth for up to four class types (<b>ct0</b>, <b>ct1</b>, <b>ct2</b>, <b>ct3</b>) per Layer 2 circuit. If you configure the class types, you must configure them in order, starting with class type <b>ct0</b>.</p> |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Bandwidth Allocation and Call Admission Control in Layer 2 Circuits on page 365</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                           |

## best-site

---

|                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                 | best-site;                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                        | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i> ]            |
| <b>Release Information</b>                                                                                                                                                                                                                                    | Statement introduced in Junos OS Release 12.2.                                                                                                                                                                                                    |
| <b>Description</b>                                                                                                                                                                                                                                            | Enables the VPLS multihoming best site functionality, allowing the site on which it has been enabled to be the preferred site for this PE router. This statement must be configured on all PE routers within the optimized VPLS routing instance. |
| <div> <b>NOTE:</b> In the VPLS documentation, the word <i>router</i> in terms such as <i>PE router</i> is used to refer to any device that provides routing functions.</div> |                                                                                                                                                                                                                                                   |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                               | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                               |
| <b>Related Documentation</b>                                                                                                                                                                                                                                  | <ul style="list-style-type: none"><li>• <a href="#">Example: VPLS Multihoming, Improved Convergence Time on page 756</a></li></ul>                                                                                                                |



## bfd-liveness-detection (Layer 2 VPN and VPLS)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> bfd-liveness-detection {     detection-time {         threshold <i>milliseconds</i>;     }     minimum-interval <i>milliseconds</i>;     minimum-receive-interval <i>milliseconds</i>;     multiplier <i>number</i>;     no-adaptation;     transmit-interval {         minimum-interval <i>milliseconds</i>;         threshold <i>milliseconds</i>;     }     version (1   automatic); } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn oam],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls oam],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn oam],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls oam]</p> |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 10.0.</p> <p>Statement introduced in Junos OS Release 13.2 for Layer 2 VPNs and VPLS.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | <p>Configure bidirectional failure detection timers.</p> <p>The BFD failure detection timers are adaptive and can be adjusted to be more or less aggressive. For example, the timers can adapt to a higher value if the adjacency fails, or a neighbor can negotiate a higher value for a timer than the configured value. The timers adapt to a higher value when a BFD session flap occurs more than three times in a span of 15 seconds. A back-off algorithm increases the receive (Rx) interval by two if the local BFD instance is the reason for the session flap. The transmission (Tx) interval is increased by two if the remote BFD instance is the reason for the session flap. You can use the <b>clear bfd adaptation</b> command to return BFD interval timers to their configured values. The <b>clear bfd adaptation</b> command is hitless, meaning that the command does not affect traffic flow on the routing device.</p> <p>The remaining statements are explained separately.</p>                             |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

- Related Documentation**
- [Configuring BFD for Layer 2 VPN and VPLS on page 186](#)
  - [Example: Configuring BFD for Static Routes](#)

---

## community (Protocols Layer 2 Circuit)

---



|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>community <i>community-name</i> {<br/>    invert-match;<br/>    members <i>community-members</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | <pre>[edit logical-systems <i>logical-system-name</i> policy-options],<br/>[edit logical-systems <i>logical-system-name</i> protocols l2circuit local-switching interface<br/>  <i>interface-name</i> backup-neighbor <i>address</i>],<br/>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i><br/>  interface <i>interface-name</i>],<br/>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface<br/>  <i>interface-name</i> backup-neighbor <i>address</i>],<br/>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols<br/>  vpls neighbor <i>address</i> backup-neighbor <i>address</i>],<br/>[edit policy-options],<br/>[edit protocols l2circuit local-switching interface <i>interface-name</i> backup-neighbor <i>address</i>],<br/>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],<br/>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> backup-neighbor <i>address</i>],<br/>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i><br/>  backup-neighbor <i>address</i>]</pre> |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Hierarchy levels associated with the <b>backup-neighbor</b> statement (pseudowire redundancy) added in Junos OS Release 9.2.</p> <p>Statement introduced in Junos OS Release 12.3 at the <b>[edit protocols l2circuit local-switching interface <i>interface-name</i> backup-neighbor <i>address</i>]</b> hierarchy level.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | Specify the community for the Layer 2 circuit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>                  | <p><b><i>community-name</i></b>—Name of the Layer 2 circuit community.</p> <p><b>invert-match</b>—Invert the results of the community expression match.</p> <p><b>members <i>community-members</i></b>—Specify the members of the community.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Layer 2 Circuit Community on page 357</a></li><li>• <a href="#">Configuring Pseudowire Redundancy on the PE Router on page 180</a></li><li>• <a href="#">Example: Configuring Layer 2 Circuit Switching Protection on page 420</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## connection-protection

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | connection-protection;                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols l2circuit local-switching interface <i>interface-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface],<br>[edit protocols l2circuit local-switching interface <i>interface-name</i> ],<br>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> ]         |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | Enable connection protection on the Layer 2 circuit. Connection protection enables you to configure a redundant pseudowire to act as a backup connection and can be configured between PE routers, maintaining Layer 2 circuit and VPLS services after certain types of failures. This feature helps to improve the reliability of networks where a single point of failure could interrupt service for customers. |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring Layer 2 Circuit Switching Protection on page 420</a></li> </ul>                                                                                                                                                                                                                                                                          |

## connectivity-type

|                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                 | connectivity-type (ce   irb   permanent);                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                        | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls]                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>                                                                                                                                                                                                                                                    | Statement introduced in Junos OS Release 9.1.<br><b>irb</b> option introduced in Junos OS Release 9.3.<br><b>permanent</b> option introduced in Junos OS Release 10.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>                                                                                                                                                                                                                                                            | Specify when a VPLS connection is taken down depending on whether or not the interface for the VPLS routing instance is customer-facing or integrated routing and bridging (IRB).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <div>  <p><b>NOTE:</b> The <b>connectivity-type</b> statement is not supported for FEC 129 VPLS (also known as LDP VPLS with BGP-based autodiscovery).</p> </div>                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Default</b>                                                                                                                                                                                                                                                                | ce                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Options</b>                                                                                                                                                                                                                                                                | <p><b>ce</b>—Require that for the VPLS connection to be up, the customer-facing interface for the VPLS routing instance must also be up. If the customer-facing interface fails, the VPLS connection is taken down.</p> <p><b>irb</b>—Allow a VPLS connection to remain up so long as an IRB interface is configured for the VPLS routing instance.</p> <p><b>permanent</b>—Allow a VPLS connection to remain up until specifically taken down. This option is reserved for use in configuring Layer 2 Wholesale subscriber networks. See the <i>Broadband Subscriber Management Solutions Guide</i> for details about configuring a Layer 2 Wholesale network.</p> |
| <div>  <p><b>NOTE:</b> To specifically take down a VPLS routing instance that is using the <b>permanent</b> option, all associated static logical interfaces must also be down.</p> </div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                               | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li><a href="#">Configuring VPLS Routing Instance and VPLS Interface Connectivity on page 572</a></li> <li><a href="#">Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                         |

## control-channel (Protocols OAM)


|                                 |                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | control-channel {<br>pwe3-control-word;<br>pw-label-ttl-1;<br>router-alert-label;<br>}                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn oam],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls oam],<br>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn oam],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls oam] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.0.                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | Configure the Virtual Circuit Connection Verification (VCCV) BFD control channel. VCCV provides a control channel associated with a pseudowire. You can configure a number of different CV types for this control channel, based on the configuration of the pseudowire.                                                                                                                                |
| <b>Options</b>                  | <p><b>pwe3-control-word</b>—For BGP-based pseudowires that send OAM packets with a control word that has 0001b as the first nibble.</p> <p><b>pw-label-ttl-1</b>—For BGP-based pseudowires that send OAM packets with the MPLS pseudowire label and time-to-live (TTL) set to 1.</p> <p><b>router-alert-label</b>—For BGP-based pseudowires that send OAM packets with router alert label.</p>          |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring BFD for VCCV for Layer 2 VPNs, Layer 2 Circuits, and VPLS on page 188</a></li> </ul>                                                                                                                                                                                                                                                   |

## control-word (Protocols Layer 2 Circuit Neighbor)

---

|                                 |                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | (control-word   no-control-word);                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> ],<br>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> ]                                                             |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                  |
| <b>Description</b>              | Specify the control word. The control word is four bytes long and is inserted between the Layer 2 protocol data unit (PDU) being transported and the virtual circuit (VC) label that is used for demultiplexing.                                                                   |
| <b>Options</b>                  | <b>control-word</b> —Enable the use of the control word.<br><b>Default:</b> A null control word is enabled by default. You can also configure the control word explicitly using the <b>control-word</b> statement.<br><b>no-control-word</b> —Disable the use of the control word. |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Control Word for Frame Relay Interfaces on page 352</a></li></ul>                                                                                                                                              |

## control-word (Protocols Layer 2 VPN)

|                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                                               | control-word;                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                                                      | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols <a href="#">l2vpn</a> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols <a href="#">l2vpn</a> ] |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                                                                                  | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                            |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                                                          | Specify the control word. The control word is 4 bytes long and is inserted between the Layer 2 protocol data unit (PDU) being transported and the virtual connection (VC) label that is used for demultiplexing.             |
| <div>  <p><b>NOTE:</b> The following configuration statements are ignored for time-division multiplexing pseudowires at the [edit protocols <a href="#">l2vpn</a>] hierarchy level:</p> <ul style="list-style-type: none"> <li>• control-word</li> <li>• no-control-word</li> </ul> </div> |                                                                                                                                                                                                                              |
| <b>Default</b>                                                                                                                                                                                                                                                                                                                                                              | The control word is enabled by default. You can also configure the control word explicitly using the <b>control-word</b> statement.                                                                                          |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                                                                             | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                          |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>• <a href="#">Disabling the Control Word for Layer 2 VPNs on page 167</a></li> <li>• <a href="#">no-control-word on page 1165</a></li> </ul>                                          |

## control-word (BGP VPLS)

---

|                                 |                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | control-word;                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls]                                                                         |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 14.1.                                                                                                                                                                                                                   |
| <b>Description</b>              | Set <b>control-word</b> to request that other routers insert a control word between the label stack and the MPLS payload.                                                                                                                                        |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Control Word for BGP VPLS Overview on page 550</a></li><li>• <a href="#">Configuring a Control Word for BGP VPLS on page 551</a></li><li>• <a href="#">no-control-word (BGP VPLS) on page 1164</a></li></ul> |

## description (Protocols Layer 2 Circuit Neighbor)

---

|                                 |                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | description <i>text</i> ;                                                                                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> ],<br>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> ] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                      |
| <b>Description</b>              | Provide a text description for the Layer 2 circuit. If the text includes one or more spaces, enclose the entire text string in quotation marks (" ").                                                                  |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Description on page 10</a></li></ul>                                                                                                               |



## description (Protocols Layer 2 VPN)

|                                 |                                                                                                                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>description text;</code>                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i> interface <i>interface-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i> interface <i>interface-name</i> ] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 11.1 for EX Series switches.                                                                                                                                                                               |
| <b>Description</b>              | Describe the VPN or virtual private LAN service (VPLS) routing instance.                                                                                                                                                                                                                                 |
| <b>Options</b>                  | <b>text</b> —Provide a text description. If the text includes one or more spaces, enclose it in quotation marks (" "). Any descriptive text you include is displayed in the output of the <b>show route instance detail</b> command and has no effect on operation.                                      |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Site on page 127</a></li> <li>• <a href="#">Configuring an MPLS-Based Layer 2 VPN (CLI Procedure)</a></li> </ul>                                                                                                                    |

## detection-time (BFD Liveness Detection)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre> detection-time {     threshold milliseconds; } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>     | <pre> [edit logical-systems <i>logical-system-name</i> protocols bgp bfd-liveness-detection], [edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i>   bfd-liveness-detection], [edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i>   bfd-liveness-detection], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   bgp bfd-liveness-detection], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   bgp group <i>group-name</i> bfd-liveness-detection], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection], [edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   l2vpn oam bfd-liveness-detection], [edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection], [edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection], [edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   vpls oam bfd-liveness-detection], [edit protocols bgp bfd-liveness-detection], [edit protocols bgp group <i>group-name</i> bfd-liveness-detection], [edit protocols bgp group <i>group-name</i> neighbor <i>address</i> bgp bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i>   bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor   <i>address</i> bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam   bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>   neighbor <i>neighbor-id</i> oam bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection] </pre> |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 8.2.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for BFD authentication introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 13.2 for Layer 2 VPNs and VPLS.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>         | <p>Enable BFD failure detection. The BFD failure detection timers are adaptive and can be adjusted to be faster or slower. The lower the BFD failure detection timer value, the faster the failure detection and vice versa. For example, the timers can adapt to a higher value if the adjacency fails (that is, the timer detects failures more slowly). Or a neighbor can negotiate a higher value for a timer than the configured value. The timers adapt to a higher value when a BFD session flap occurs more than three times in a span of 15 seconds.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

A back-off algorithm increases the receive (Rx) interval by two if the local BFD instance is the reason for the session flap. The transmission (Tx) interval is increased by two if the remote BFD instance is the reason for the session flap. You can use the **clear bfd adaptation** command to return BFD interval timers to their configured values. The **clear bfd adaptation** command is hitless, meaning that the command does not affect traffic flow on the routing device.

The remaining statement is explained separately.

|                                 |                                                                        |
|---------------------------------|------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.                   |
|                                 | routing-control—To add this statement to the configuration.            |
| <b>Related Documentation</b>    | • <a href="#">Configuring BFD for Layer 2 VPN and VPLS on page 186</a> |
|                                 | • <i>Example: Configuring BFD for BGP</i>                              |
|                                 | • <i>bfd-liveness-detection</i>                                        |
|                                 | • <a href="#">threshold on page 1205</a>                               |

## encapsulation (Logical Interface)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | encapsulation (atm-ccc-cell-relay   atm-ccc-vc-mux   atm-cisco-nlpid   atm-mlppp-llc   atm-nlpid   atm-ppp-llc   atm-ppp-vc-mux   atm-snap   atm-tcc-snap   atm-tcc-vc-mux   atm-vc-mux   ether-over-atm-llc   ether-vpls-over-atm-llc   ether-vpls-over-fr   ether-vpls-over-ppp   ethernet   ethernet-ccc   ethernet-vpls   ethernet-vpls-fr   frame-relay-ccc   frame-relay-ether-type   frame-relay-ether-type-tcc   frame-relay-ppp   frame-relay-tcc   gre-fragmentation   multilink-frame-relay-end-to-end   multilink-ppp   ppp-over-ether   ppp-over-ether-over-atm-llc   vlan-bridge   vlan-ccc   vlan-vci-ccc   vlan-tcc   vlan-vpls   vxlan);                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>     | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ],<br>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ],<br>[edit interfaces rlsq <i>number</i> unit <i>logical-unit-number</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers ( <b>ethernet</b> , <b>vlan-ccc</b> , and <b>vlan-tcc</b> options only).<br>Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Access Routers. Only the <b>atm-ccc-cell-relay</b> and <b>atm-ccc-vc-mux</b> options are supported on ACX Series routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>         | Configure a logical link-layer encapsulation type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Options</b>             | <p><b>atm-ccc-cell-relay</b>—Use ATM cell-relay encapsulation.</p> <p><b>atm-ccc-vc-mux</b>—Use ATM virtual circuit (VC) multiplex encapsulation on CCC circuits. When you use this encapsulation type, you can configure the <b>ccc</b> family only.</p> <p><b>atm-cisco-nlpid</b>—Use Cisco ATM network layer protocol identifier (NLPID) encapsulation. When you use this encapsulation type, you can configure the <b>inet</b> family only.</p> <p><b>atm-mlppp-llc</b>—For ATM2 IQ interfaces only, use Multilink Point-to-Point (MLPPP) over AAL5 LLC. For this encapsulation type, your router must be equipped with a Link Services or Voice Services PIC. MLPPP over ATM encapsulation is not supported on ATM2 IQ OC48 interfaces.</p> <p><b>atm-nlpid</b>—Use ATM NLPID encapsulation. When you use this encapsulation type, you can configure the <b>inet</b> family only.</p> <p><b>atm-ppp-llc</b>—(ATM2 IQ interfaces and MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP only) Use PPP over AAL5 LLC encapsulation.</p> <p><b>atm-ppp-vc-mux</b>—(ATM2 IQ interfaces and MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP only) Use PPP over ATM AAL5 multiplex encapsulation.</p> <p><b>atm-snap</b>—(All interfaces including MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP) Use ATM subnetwork attachment point (SNAP) encapsulation.</p> <p><b>atm-tcc-snap</b>—Use ATM SNAP encapsulation on translational cross-connect (TCC) circuits.</p> |

**atm-tcc-vc-mux**—Use ATM VC multiplex encapsulation on TCC circuits. When you use this encapsulation type, you can configure the **tcc** family only.

**atm-vc-mux**—(All interfaces including MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP) Use ATM VC multiplex encapsulation. When you use this encapsulation type, you can configure the **inet** family only.

**ether-over-atm-llc**—(All IP interfaces including MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP) For interfaces that carry IP traffic, use Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces.

**ether-vpls-over-atm-llc**—For ATM2 IQ interfaces only, use the Ethernet virtual private LAN service (VPLS) over ATM LLC encapsulation to bridge Ethernet interfaces and ATM interfaces over a VPLS routing instance (as described in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*). Packets from the ATM interfaces are converted to standard ENET2/802.3 encapsulated Ethernet frames with the frame check sequence (FCS) field removed.

**ether-vpls-over-fr**—For E1, T1, E3, T3, and SONET interfaces only, use the Ethernet virtual private LAN service (VPLS) over Frame Relay encapsulation to support Bridged Ethernet over Frame Relay encapsulated TDM interfaces for VPLS applications, per RFC 2427, *Multiprotocol Interconnect over Frame Relay*.



**NOTE:** The SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, the Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, and the DS3/E3 MIC do not support Ethernet over Frame Relay encapsulation.

**ether-vpls-over-ppp**—For E1, T1, E3, T3, and SONET interfaces only, use the Ethernet virtual private LAN service (VPLS) over Point-to-Point Protocol (PPP) encapsulation to support Bridged Ethernet over PPP-encapsulated TDM interfaces for VPLS applications.

**ethernet**—Use Ethernet II encapsulation (as described in RFC 894, *A Standard for the Transmission of IP Datagrams over Ethernet Networks*).

**ethernet-ccc**—Use Ethernet CCC encapsulation on Ethernet interfaces.

**ethernet-vpls**—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard Tag Protocol ID (TPID) values.



**NOTE:** The built-in Gigabit Ethernet PIC on an M7i router does not support extended VLAN VPLS encapsulation.

**ethernet-vpls-fr**—Use in a VPLS setup when a CE device is connected to a PE device over a time-division multiplexing (TDM) link. This encapsulation type enables the PE device to terminate the outer layer 2 Frame Relay connection, use the 802.1p bits inside the inner Ethernet header to classify the packets, look at the MAC address from the Ethernet header, and use the MAC address to forward the packet into a given VPLS instance.

**frame-relay-ccc**—Use Frame Relay encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

**frame-relay-ether-type**—Use Frame Relay ether type encapsulation for compatibility with Cisco Frame Relay. The physical interface must be configured with flexible-frame-relay encapsulation.

**frame-relay-ether-type-tcc**—Use Frame Relay ether type TCC for Cisco-compatible Frame Relay on TCC circuits to connect different media. The physical interface must be configured with flexible-frame-relay encapsulation.

**frame-relay-ppp**—Use PPP over Frame Relay circuits. When you use this encapsulation type, you can configure the **ppp** family only.

**frame-relay-tcc**—Use Frame Relay encapsulation on TCC circuits for connecting different media. When you use this encapsulation type, you can configure the **tcc** family only.

**gre-fragmentation**—For adaptive services interfaces only, use GRE fragmentation encapsulation to enable fragmentation of IPv4 packets in GRE tunnels. This encapsulation clears the do not fragment (DF) bit in the packet header. If the packet's size exceeds the tunnel's maximum transmission unit (MTU) value, the packet is fragmented before encapsulation.

**multilink-frame-relay-end-to-end**—Use MLFR FRF.15 encapsulation. This encapsulation is used only on multilink, link services, and voice services interfaces and their constituent T1 or E1 interfaces, and is supported on LSQ and redundant LSQ interfaces.

**multilink-ppp**—Use MLPPP encapsulation. This encapsulation is used only on multilink, link services, and voice services interfaces and their constituent T1 or E1 interfaces.

**ppp-over-ether**—You use PPP over Ethernet encapsulation to configure an underlying Ethernet interface for a dynamic PPPoE logical interface.

**ppp-over-ether-over-atm-llc**—(MX Series routers with MPCs using the ATM MIC with SFP only) For underlying ATM interfaces, use PPP over Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead, configure the interface address on the PPP interface.

**vlan-bridge**—Use Ethernet VLAN bridge encapsulation on Ethernet interfaces that have IEEE 802.1Q tagging, flexible-ethernet-services, and bridging enabled and that must accept packets carrying TPID 0x8100 or a user-defined TPID.

**vlan-ccc**—Use Ethernet virtual LAN (VLAN) encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

**vlan-vci-ccc**—Use ATM-to-Ethernet interworking encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

**vlan-tcc**—Use Ethernet VLAN encapsulation on TCC circuits. When you use this encapsulation type, you can configure the **tcc** family only.

**vlan-vpls**—Use Ethernet VLAN encapsulation on VPLS circuits.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- *Configuring Layer 2 Switching Cross-Connects Using CCC*
- *Configuring the Encapsulation for Layer 2 Switching TCCs*
- *Configuring Interface Encapsulation on Logical Interfaces*
- *Configuring MPLS LSP Tunnel Cross-Connects Using CCC*
- *Circuit and Translational Cross-Connects Overview*
- *Identifying the Access Concentrator*
- *Configuring ATM Interface Encapsulation*
- *Configuring VLAN and Extended VLAN Encapsulation*
- *Configuring ATM-to-Ethernet Interworking*
- *Configuring Interface Encapsulation on PTX Series Packet Transport Routers*
- [Configuring CCC Encapsulation for Layer 2 VPNs on page 163](#)
- [Configuring TCC Encapsulation for Layer 2 VPNs and Layer 2 Circuits on page 164](#)
- *Configuring ATM for Subscriber Access*
- *CoS on ATM IMA Pseudowire Interfaces Overview*
- *Configuring Policing on an ATM IMA Pseudowire*

## encapsulation (Physical Interface)

---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>encapsulation (atm-ccc-cell-relay   atm-pvc   cisco-hdlc   cisco-hdlc-ccc   cisco-hdlc-tcc   ethernet-bridge   ethernet-ccc   ethernet-over-atm   ethernet-tcc   ethernet-vpls   ethernet-vpls-fr   ether-vpls-over-atm-llc   ethernet-vpls-ppp   extended-frame-relay-ccc   extended-frame-relay-ether-type-tcc   extended-frame-relay-tcc   extended-vlan-bridge   extended-vlan-ccc   extended-vlan-tcc   extended-vlan-vpls   flexible-ethernet-services   flexible-frame-relay   frame-relay   frame-relay-ccc   frame-relay-ether-type   frame-relay-ether-type-tcc   frame-relay-port-ccc   frame-relay-tcc   generic-services   multilink-frame-relay-uni-nni   ppp   ppp-ccc   ppp-tcc   vlan-ccc   vlan-vci-ccc   vlan-vpls);</code>                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>     | <code>[edit interfaces <i>interface-name</i>],</code><br><code>[edit interfaces rlsq <i>number:number</i>]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 11.1 for EX Series switches.<br>Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers ( <b>flexible-ethernet-services</b> , <b>ethernet-ccc</b> , and <b>ethernet-tcc</b> options only).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b>         | Specify the physical link-layer encapsulation type. Not all encapsulation types are supported on the switches. See the switch CLI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Default</b>             | For SONET interfaces— <b>ppp</b><br><br>For ATM interfaces— <b>atm-pvc</b><br><br>For DS1, E1, and T1 interfaces— <b>ppp</b><br><br>For DS3, E3, and T3 interfaces— <b>ppp</b><br><br>For all channelized interfaces— <b>ppp</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>             | <b>atm-ccc-cell-relay</b> —Use ATM cell-relay encapsulation.<br><br><b>atm-pvc</b> —Use ATM PVC encapsulation.<br><br><b>cisco-hdlc</b> —Use Cisco-compatible High-Level Data Link Control (HDLC) framing.<br><br><b>cisco-hdlc-ccc</b> —Use Cisco-compatible HDLC framing on CCC circuits.<br><br><b>cisco-hdlc-tcc</b> —Use Cisco-compatible HDLC framing on TCC circuits for connecting different media.<br><br><b>ethernet-bridge</b> —Use Ethernet bridge encapsulation on Ethernet interfaces that have bridging enabled and that must accept all packets.<br><br><b>ethernet-ccc</b> —Use Ethernet CCC encapsulation on Ethernet interfaces that must accept packets carrying standard Tag Protocol ID (TPID) values. For 8-port, 12-port, and 48-port Fast Ethernet PICs, CCC is not supported.<br><br><b>ethernet-over-atm</b> —For interfaces that carry IPv4 traffic, use Ethernet over ATM encapsulation. When you use this encapsulation type, you cannot configure multipoint |



interfaces. As defined in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, this encapsulation type allows ATM interfaces to connect to devices that support only bridge protocol data units (BPDUs). Junos OS does not completely support bridging, but accepts BPDU packets as a default gateway. If you use the router as an edge device, then the router acts as a default gateway. It accepts Ethernet LLC/SNAP frames with IP or ARP in the payload, and drops the rest. For packets destined to the Ethernet LAN, a route lookup is done using the destination IP address. If the route lookup yields a full address match, the packet is encapsulated with an LLC/SNAP and MAC header, and the packet is forwarded to the ATM interface.

**ethernet-tcc**—For interfaces that carry IPv4 traffic, use Ethernet TCC encapsulation on interfaces that must accept packets carrying standard TPID values. For 8-port, 12-port, and 48-port Fast Ethernet PICs, TCC is not supported.

**ethernet-vpls**—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard TPID values. On M Series routers, except the M320 router, the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.

**ethernet-vpls-fr**—Use in a VPLS setup when a CE device is connected to a PE device over a time division multiplexing (TDM) link. This encapsulation type enables the PE device to terminate the outer Layer 2 Frame Relay connection, use the 802.1p bits inside the inner Ethernet header to classify the packets, look at the MAC address from the Ethernet header, and use the MAC address to forward the packet into a given VPLS instance.

**ethernet-vpls-ppp**—Use in a VPLS setup when a CE device is connected to a PE device over a time division multiplexing (TDM) link. This encapsulation type enables the PE device to terminate the outer Layer 2 PPP connection, use the 802.1p bits inside the inner Ethernet header to classify the packets, look at the MAC address from the Ethernet header, and use it to forward the packet into a given VPLS instance.

**ether-vpls-over-atm-llc**—For ATM intelligent queuing (IQ) interfaces only, use the Ethernet virtual private LAN service (VPLS) over ATM LLC encapsulation to bridge Ethernet interfaces and ATM interfaces over a VPLS routing instance (as described in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*). Packets from the ATM interfaces are converted to standard ENET2/802.3 encapsulated Ethernet frames with the frame check sequence (FCS) field removed.

**extended-frame-relay-ccc**—Use Frame Relay encapsulation on CCC circuits. This encapsulation type allows you to dedicate DLCIs 1 through 1022 to CCC.

**extended-frame-relay-ether-type-tcc**—Use extended Frame Relay ether type TCC for Cisco-compatible Frame Relay for DLCIs 1 through 1022. This encapsulation type is used for circuits with different media on either side of the connection.

**extended-frame-relay-tcc**—Use Frame Relay encapsulation on TCC circuits to connect different media. This encapsulation type allows you to dedicate DLCIs 1 through 1022 to TCC.

**extended-vlan-bridge**—Use extended VLAN bridge encapsulation on Ethernet interfaces that have IEEE 802.1Q VLAN tagging and bridging enabled and that must accept packets carrying TPID 0x8100 or a user-defined TPID.

**extended-vlan-ccc**—Use extended VLAN encapsulation on CCC circuits with Gigabit Ethernet and 4-port Fast Ethernet interfaces that must accept packets carrying 802.1Q values. For 8-port, 12-port, and 48-port Fast Ethernet PICs, extended VLAN CCC is not supported. For 4-port Gigabit Ethernet PICs, extended VLAN CCC is not supported.

**extended-vlan-tcc**—For interfaces that carry IPv4 traffic, use extended VLAN encapsulation on TCC circuits with Gigabit Ethernet interfaces on which you want to use 802.1Q tagging. For 4-port Gigabit Ethernet PICs, extended VLAN TCC is not supported.

**extended-vlan-vpls**—Use extended VLAN VPLS encapsulation on Ethernet interfaces that have VLAN 802.1Q tagging and VPLS enabled and that must accept packets carrying TPIDs 0x8100, 0x9100, and 0x9901. On M Series routers, except the M320 router, the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.



**NOTE:** The built-in Gigabit Ethernet PIC on an M7i router does not support extended VLAN VPLS encapsulation.

---

**flexible-ethernet-services**—For Gigabit Ethernet IQ interfaces and Gigabit Ethernet PICs with small form-factor pluggable transceivers (SFPs) (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), use flexible Ethernet services encapsulation when you want to configure multiple per-unit Ethernet encapsulations. Aggregated Ethernet bundles can use this encapsulation type. This encapsulation type allows you to configure any combination of route, TCC, CCC, Layer 2 virtual private networks (VPNs), and VPLS encapsulations on a single physical port. If you configure flexible Ethernet services encapsulation on the physical interface, VLAN IDs from 1 through 511 are no longer reserved for normal VLANs.

**flexible-frame-relay**—For IQ interfaces only, use flexible Frame Relay encapsulation when you want to configure multiple per-unit Frame Relay encapsulations. This encapsulation type allows you to configure any combination of TCC, CCC, and standard Frame Relay encapsulations on a single physical port. Also, each logical interface can have any DLCI value from 1 through 1022.

**frame-relay**—Use Frame Relay encapsulation.

**frame-relay-ccc**—Use Frame Relay encapsulation on CCC circuits.

**frame-relay-ether-type**—Use Frame Relay ether type encapsulation for compatibility with the Cisco Frame Relay.

**frame-relay-ether-type-tcc**—Use Frame Relay ether type TCC for Cisco-compatible Frame Relay on TCC circuits to connect different media.

**frame-relay-port-ccc**—Use Frame Relay port CCC encapsulation to transparently carry all the DLCIs between two customer edge (CE) routers without explicitly configuring each DLCI on the two provider edge (PE) routers with Frame Relay transport. When you use this encapsulation type, you can configure the **ccc** family only.

**frame-relay-tcc**—Use Frame Relay encapsulation on TCC circuits to connect different media.

**generic-services**—Use generic services encapsulation for services with a hierarchical scheduler.

**multilink-frame-relay-uni-nni**—Use MLFR UNI NNI encapsulation. This encapsulation is used on link services, voice services interfaces functioning as FRF.16 bundles, and their constituent T1 or E1 interfaces, and is supported on LSQ and redundant LSQ interfaces.

**ppp**—Use serial PPP encapsulation.

**ppp-ccc**—Use serial PPP encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

**ppp-tcc**—Use serial PPP encapsulation on TCC circuits for connecting different media. When you use this encapsulation type, you can configure the **tcc** family only.

**vlan-ccc**—Use Ethernet VLAN encapsulation on CCC circuits.

**vlan-vci-ccc**—Use ATM-to-Ethernet interworking encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only. All logical interfaces configured on the Ethernet interface must also have the encapsulation type set to **vlan-vci-ccc**.

**vlan-vpls**—Use VLAN VPLS encapsulation on Ethernet interfaces with VLAN tagging and VPLS enabled. Interfaces with VLAN VPLS encapsulation accept packets carrying standard TPID values only. On M Series routers, except the M320 router, the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.



#### NOTE:

- Label-switched interfaces (LSIs) do not support VLAN VPLS encapsulation. Therefore, you can only use VLAN VPLS encapsulation on a PE-router-to-CE-router interface and not a core-facing interface.
- Starting with Junos OS release 13.3, a commit error occurs when you configure **vlan-vpls** encapsulation on a physical interface and configure family **inet** on one of the logical units. Previously, it was possible to commit this invalid configuration.

|                                 |                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | <b>interface</b> —To view this statement in the configuration.<br><b>interface-control</b> —To add this statement to the configuration. |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|

**Related  
Documentation**

- *Configuring Interface Encapsulation on Physical Interfaces*
- [Configuring CCC Encapsulation for Layer 2 VPNs on page 163](#)
- *Configuring Layer 2 Switching Cross-Connects Using CCC*
- [Configuring TCC Encapsulation for Layer 2 VPNs and Layer 2 Circuits on page 164](#)
- *Configuring ATM Interface Encapsulation*
- *Configuring ATM-to-Ethernet Interworking*
- *Configuring VLAN and Extended VLAN Encapsulation*
- *OBSOLETE: Configuring Extended VLAN Encapsulation*
- *Configuring Encapsulation for Layer 2 Wholesale VLAN Interfaces*
- [Configuring Interfaces for Layer 2 Circuits on page 350](#)
- *Configuring Interface Encapsulation on PTX Series Packet Transport Routers*
- *Configuring MPLS LSP Tunnel Cross-Connects Using CCC*
- *Configuring TCC*
- [Configuring VPLS Interface Encapsulation on page 604](#)
- [Configuring Interfaces for VPLS Routing on page 603](#)
- *Defining the Encapsulation for Switching Cross-Connects*

## encapsulation-type (Layer 2 Circuits)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | encapsulation-type (atm-aal5   atm-cell   atm-cell-port-mode   atm-cell-vc-mode   atm-cell-vp-mode   cesop   cisco-hdlc   ethernet   ethernet-vlan   frame-relay   frame-relay-port-mode   interworking   ppp   satop-e1   satop-e3   satop-t1   satop-t3);                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols l2circuit local-switching interface <i>interface-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> ],<br>[edit protocols l2circuit local-switching interface <i>interface-name</i> ],<br>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Specify the type of Layer 2 traffic transiting the Layer 2 circuit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <p><b>atm-aal5</b>—ATM Adaptation Layer (AAL/5)</p> <p><b>atm-cell</b>—ATM cell relay</p> <p><b>atm-cell-port-mode</b>—ATM cell relay port promiscuous mode</p> <p><b>atm-cell-vc-mode</b>—ATM VC cell relay nonpromiscuous mode</p> <p><b>atm-cell-vp-mode</b>—ATM virtual path (VP) cell relay promiscuous mode</p> <p><b>cesop</b>—CESOP-based Layer 2 circuit</p> <p><b>cisco-hdlc</b>—Cisco Systems-compatible HDLC</p> <p><b>ethernet</b>—Ethernet</p> <p><b>ethernet-vlan</b>—Ethernet VLAN</p> <p><b>frame-relay</b>—Frame Relay</p> <p><b>frame-relay-port-mode</b>—Frame Relay port mode</p> <p><b>interworking</b>—Layer 2.5 interworking</p> <p><b>ppp</b>—PPP</p> <p><b>satop-e1</b>—SATSOP-E1-based Layer 2 circuit</p> <p><b>satop-e3</b>—SATSOP-E3-based Layer 2 circuit</p> <p><b>satop-t1</b>—SATSOP-T1-based Layer 2 circuit</p> <p><b>satop-t3</b>—SATSOP-T3-based Layer 2 circuit</p> |
| <b>Required Privilege Level</b> | <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 Encapsulation Type for the Layer 2 Circuit Neighbor Interface on page 353](#)

## encapsulation-type (Layer 2 VPNs)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | encapsulation-type (atm-aal5   atm-cell   atm-cell-port-mode   atm-cell-vc-mode   atm-cell-vp-mode   cesop   cisco-hdlc   ethernet   ethernet-vlan   frame-relay   frame-relay-port-mode   interworking   ppp   satop-e1   satop-e3   satop-t1   satop-t3);                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>     | <p>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn neighbor <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls],</p> <p>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn neighbor <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i>]</p> |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 9.2.</p> <p>Statement introduced in Junos OS Release 11.1 for EX Series switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>         | Specify the type of Layer 2 traffic originating from the CE device. Only the <b>ethernet</b> and <b>ethernet-vlan</b> encapsulation types are supported for VPLS. Not all encapsulation types are supported on the switches. See the switch CLI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>             | <p><b>atm-aal5</b>—ATM Adaptation Layer (AAL/5)</p> <p><b>atm-cell</b>—ATM cell relay</p> <p><b>atm-cell-port-mode</b>—ATM cell relay port promiscuous mode</p> <p><b>atm-cell-vc-mode</b>—ATM VC cell relay nonpromiscuous mode</p> <p><b>atm-cell-vp-mode</b>—ATM virtual path (VP) cell relay promiscuous mode</p> <p><b>cesop</b>—CESOP-based Layer 2 VPN</p> <p><b>cisco-hdlc</b>—Cisco Systems-compatible HDLC</p> <p><b>ethernet</b>—Ethernet</p> <p><b>ethernet-vlan</b>—Ethernet VLAN</p> <p><b>frame-relay</b>—Frame Relay</p> <p><b>frame-relay-port-mode</b>—Frame Relay port mode</p> <p><b>interworking</b>—Layer 2.5 interworking VPN</p> <p><b>ppp</b>—PPP</p> <p><b>satsop-e1</b>—SATSOP-E1-based Layer 2 VPN</p>                                                                                                                                                                                                                                                                      |

**satsop-e3**—SATSOP-E3-based Layer 2 VPN

**satsop-t1**—SATSOP-T1-based Layer 2 VPN

**satsop-t3**—SATSOP-T3-based Layer 2 VPN

**Default:** For VPLS networks, the default encapsulation type is **ethernet**.

**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring the Encapsulation Type on page 129](#)
- [Configuring VPLS Routing Instances on page 563](#)
- [Configuring the Encapsulation Type for the Layer 2 Circuit Neighbor Interface on page 353](#)
- [Configuring an MPLS-Based Layer 2 VPN \(CLI Procedure\)](#)

---

## egress-protection (Layer 2 circuit)

---

**Syntax**

```
egress-protection {
 protected-l2circuit {
 egress-pe address;
 ingress-pe address;
 virtual-circuit-id identifier;
 }
 protector-interface interface-name;
 protector-pe address {
 context-identifier identifier;
 lsp lsp-name;
 }
}
```

**Hierarchy Level** [edit logical-systems *logical-system-name* protocols l2circuit neighbor *address* interface *interface-name*],  
[edit protocols l2circuit neighbor *address* interface *interface-name*]

**Release Information** Statement introduced in Junos OS release 10.4.

**Description** Configures an egress protection virtual circuit (EPVC).

**Options** The other 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**

- [Example: Configuring an Egress Protection LSP for a Layer 2 Circuit on page 404](#)



## egress-protection (MPLS)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>egress-protection {     context-identifier <i>context-id</i> {         primary   protector;         metric <i>igp-metric-value</i>;         advertise-mode (stub-alias   stub-proxy);     } }</pre>                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols mpls],<br>[edit logical-systems <i>logical-system-name</i> protocols mpls label-switched-path <i>lsp-name</i> ],<br>[edit protocols mpls],<br>[edit protocols mpls label-switched-path <i>lsp-name</i> ]                                                                                                                         |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.4.<br>Options <b>primary</b> , <b>protector</b> , and <b>metric</b> introduced in Junos OS Release 11.4R3.<br>Option <b>advertise-mode</b> introduced in Junos OS Release 13.3.                                                                                                                                                                 |
| <b>Description</b>              | Enables an Edge Protection Virtual Circuit (EPVC) for the MPLS protocol.                                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <p><b>context-identifier <i>context-id-ip-address</i></b>—(Optional) The context identifier IPv4 address.</p> <p><b>metric <i>igp-metric-value</i></b>—(Optional) The IGP metric value ranging from 2 through 16777215.</p> <p><b>(primary   protector)</b>—On the primary PE router, configure as type <b>primary</b>. On the protector PE router, configure as type <b>protector</b>.</p> |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Example: Configuring Egress Protection for Layer 3 VPN Services</i></li> <li>• <i>Example: Configuring Layer 3 VPN Egress Protection with RSVP and LDP</i></li> </ul>                                                                                                                                                                           |

## end-interface

---

|                            |                                                                                                                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre>end-interface {<br/>    interface <i>interface-name</i>;<br/>    no-revert;<br/>    protect-interface <i>interface-name</i>;<br/>}</pre>                                                          |
| <b>Hierarchy Level</b>     | [edit logical-systems <i>logical-system-name</i> protocols l2circuit local-switching interface <i>interface-name</i> ],<br>[edit protocols l2circuit local-switching interface <i>interface-name</i> ] |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.                                                                                                                                                      |
| <b>Description</b>         | Specify the end interface for a local interface switch.                                                                                                                                                |



**NOTE:** The protect interface must be configured prior to configuring the no-revert statement.

---

The remaining statements are explained separately.

|                                 |                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Local Interface Switching in Layer 2 Circuits on page 348</a></li></ul> |

## esi

**Syntax** *esi identifier* {  
     esi-mode all active | single-active;  
 }

**Hierarchy Level** [edit interfaces *interface-name*]

**Release Information** Statement introduced in Junos OS Release 14.1.

**Description** Configure the Ethernet Segment Identifier (ESI) value for the multihomed interfaces.

**Options** *esi*—Ten octet value. ESI value 0 and all fixed filters are reserved, and not used for configuring a multihomed Ethernet segment.



## NOTE:

- Two interfaces in the same EVPN instance (EVI) cannot be configured with the same ESI value.
- The left most octet must be configured as 00. The other 9 octets are fully configurable

**single-active**—Configure the EVPN active-standby multihoming mode of operation.

**Required Privilege** interface—To view this statement in the configuration.

**Level** interface-control—To add this statement to the configuration.

**Related Documentation** • *evpn*

## extended-vlan-list

---

|                                 |                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>extended-vlan-list <i>vlan-id</i>   [<i>vlan-id set</i>];</code>                                                                                        |
| <b>Hierarchy Level</b>          | <code>[edit routing-instances <i>routing-instance-name</i> instance-type virtual-switch protocols evpn]</code>                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 14.1.<br>Statement introduced in Junos OS Release 14.2 on EX Series switches.                                        |
| <b>Description</b>              | Specify the VLAN or range of VLANs that are extended over the WAN, wherein all the single VLAN bridge domains corresponding to these VLANs are stretched.     |
| <b>Options</b>                  | <b><i>vlan-id</i></b> —VLAN ID to be EVPN extended.<br><b><i>vlan-id set</i></b> —List of VLAN IDs to be EVPN extended.<br><b>Range:</b> 1 through 4094 VLANs |
| <b>Required Privilege Level</b> | <b>routing</b> —To view this statement in the configuration.<br><b>routing-control</b> —To add this statement to the configuration.                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>evpn</i></li></ul>                                                                                                 |

## family

```

Syntax family {
 (inet | inet6 | inet-vpn | inet6-vpn | iso-vpn) {
 (any | flow | labeled-unicast | multicast | unicast) {
 accepted-prefix-limit {
 maximum number;
 teardown <percentage-threshold> idle-timeout (forever | minutes);
 }
 add-path {
 send {
 path-count number;
 prefix-policy [policy-names];
 }
 receive;
 }
 algp [disable];
 loops number;
 prefix-limit {
 maximum number;
 teardown <percentage> <idle-timeout (forever | minutes)>;
 }
 protection;
 rib-group group-name;
 topology name {
 community {
 target identifier;
 }
 }
 flow {
 no-install;
 no-validate policy-name;
 }
 labeled-unicast {
 accepted-prefix-limit {
 maximum number;
 teardown <percentage> <idle-timeout (forever | minutes)>;
 }
 aggregate-label {
 community community-name;
 }
 explicit-null {
 connected-only;
 }
 prefix-limit {
 maximum number;
 teardown <percentage> <idle-timeout (forever | minutes)>;
 }
 resolve-vpn;
 rib inet.3;
 rib-group group-name;
 traffic-statistics {
 file filename <world-readable | no-world-readable>;
 interval seconds;
 }
 }
 }
 }
}

```

```

 }
 }
}
route-target {
 accepted-prefix-limit {
 maximum number;
 proxy-generate <route-target-policy route-target-policy-name>;
 teardown <percentage> <idle-timeout (forever | minutes)>;
 }
 advertise-default;
 external-paths number;
 prefix-limit {
 maximum number;
 teardown <percentage> <idle-timeout (forever | minutes)>;
 }
}
(inet-mdt | inet-mvpn | inet6-mvpn | l2vpn) {
 signaling {
 accepted-prefix-limit {
 maximum number;
 teardown <percentage-threshold> idle-timeout (forever | minutes);
 }
 }
 add-path {
 send {
 path-count number;
 prefix-policy [policy-names];
 }
 receive;
 }
 aigp [disable];
 damping;
 loops number;
 prefix-limit {
 maximum number;
 teardown <percentage> <idle-timeout (forever | minutes)>;
 }
 rib-group group-name;
}
}
traffic-engineering;
}

```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hierarchy Level</b>     | <p>[edit logical-systems <i>logical-system-name</i> protocols bgp],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i>],</p> <p>[edit protocols bgp],</p> <p>[edit protocols bgp group <i>group-name</i>],</p> <p>[edit protocols bgp group <i>group-name</i> neighbor <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i>]</p> |
| <b>Release Information</b> | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> <p><b>inet-mvpn</b> and <b>inet6-mvpn</b> statements introduced in Junos OS Release 8.4.</p> <p><b>inet-mdt</b> statement introduced in Junos OS Release 9.4.</p> <p>Support for the <b>loops</b> statement introduced in Junos OS Release 9.6.</p> <p><b>evpn</b> statement introduced in Junos OS Release 13.2.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> <p><b>traffic-engineering</b> statement introduced in Junos OS Release 14.2.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>         | <p>Enable multiprotocol BGP (MP-BGP) by configuring BGP to carry network layer reachability information (NLRI) for address families other than unicast IPv4, to specify MP-BGP to carry NLRI for the IPv6 address family, or to carry NLRI for VPNs.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

- Options**
- any**—Configure the family type to be both unicast and multicast.
  - evpn**—Configure NLRI parameters for Ethernet VPNs (EVPNs).
  - inet**—Configure NLRI parameters for IPv4.
  - inet6**—Configure NLRI parameters for IPv6.
  - inet-mdt**—Configure NLRI parameters for the multicast distribution tree (MDT) subaddress family identifier (SAFI) for IPv4 traffic in Layer 3 VPNs.
  - inet-mvpn**—Configure NLRI parameters for IPv4 for multicast VPNs.
  - inet6-mvpn**—Configure NLRI parameters for IPv6 for multicast VPNs.
  - inet-vpn**—Configure NLRI parameters for IPv4 for Layer 3 VPNs.
  - inet6-vpn**—Configure NLRI parameters for IPv6 for Layer 3 VPNs.
  - inet6-vpn**—Configure NLRI parameters for IPv6 for Layer 3 VPNs.
  - iso-vpn**—Configure NLRI parameters for IS-IS for Layer 3 VPNs.
  - l2vpn**—Configure NLRI parameters for IPv4 for MPLS-based Layer 2 VPNs and VPLS.
  - labeled-unicast**—Configure the family type to be labeled-unicast. This means that the BGP peers are being used only to carry the unicast routes that are being used by labeled-unicast for resolving the labeled-unicast routes. This statement is supported only with **inet** and **inet6**.
  - multicast**—Configure the family type to be multicast. This means that the BGP peers are being used only to carry the unicast routes that are being used by multicast for resolving the multicast routes.
  - unicast**—Configure the family type to be unicast. This means that the BGP peers only carry the unicast routes that are being used for unicast forwarding purposes. The default family type is **unicast**.

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**

- [Configuring IBGP Sessions Between PE Routers in VPNs on page 19](#)
- *Understanding Multiprotocol BGP*
- *autonomous-system*
- *local-as*
- *Understanding Multiprotocol BGP*



## family multiservice

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre> family multiservice {     destination-mac;     label-1;     label-2;     payload {         ip {             layer-3 {                 (source-ip-only   destination-ip-only);             }             layer-3-only;             layer-4;         }     }     source-mac;     symmetric-hash {         complement;     } } </pre>                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>     | [edit forwarding-options hash-key]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 8.0.</p> <p><b>ip</b>, <b>label-1</b>, <b>label-2</b>, <b>layer-3-only</b>, and <b>payload</b> options introduced in Junos OS Release 9.4.</p> <p><b>layer-3</b>, <b>layer-4</b>, <b>source-ip-only</b>, and <b>destination-ip-only</b> options introduced in Junos OS Release 9.5.</p> <p><b>symmetric-hash</b> and <b>complement</b> options introduced in Junos OS Release 9.6.</p>                                                                                                                                                                                                                                                                             |
| <b>Description</b>         | <p>Configure load balancing based on Layer 2 media access control information. On MX Series routers, configure VPLS load balancing. On M120 and M320 routers only, configure VPLS load balancing based on MPLS labels and IP information. For IPv4 traffic, only the IP source and destination addresses are included in the hash key. For MPLS and IPv4 traffic, one or two MPLS labels and IPv4 source and destination addresses are included. For MPLS Ethernet pseudowires, only one or two MPLS labels are included in the hash key.</p>                                                                                                                                                                  |
| <b>Options</b>             | <p>You can configure one or more options to load-balance using the packet information that you specify.</p> <p><b>destination-mac</b>—Include the destination-address MAC information in the hash key for Layer 2 load balancing.</p> <p><b>label-1</b> (M120 and M320 routers only)—Include the first MPLS label in the hash key. Used for including a one-label packet for per-flow load balancing of IPv4 VPLS traffic based on IP information and MPLS labels.</p> <p><b>label-2</b> (M120 and M320 routers only)—Include the second MPLS label in the hash key. If both <b>label-1</b> and <b>label-2</b> are specified, the entire first label and the first 16 bits of the second label are hashed.</p> |

**payload** (MX Series, M120, and M320 routers only)—Include the packet's IP payload in the hash key.

- **ip** (MX Series, M120, and M320 routers only)—Include the IP address of the IPv4 or IPv6 payload in the hash key.
- **layer-3** (MX Series routers only)—Use this to include Layer 3 information from the packet's IP payload in the hash key.
  - **destination-ip-only** (MX Series routers only)—Use this to include only the destination IP address in the payload in the hash key.
  - **source-ip-only** (MX Series routers only)—Use this to include only the source IP address in the payload in the hash key.



**NOTE:** You can include either the **source-ip-only** or the **destination-ip-only** statement, not both. They are mutually exclusive.

---

- **layer-3-only** (M120, and M320 routers only)—Include only the Layer 3 information from the packet's IP payload in the hash key.
- **layer-4** (MX Series routers only)—Include Layer 4 information from the packet's IP payload in the hash key.



**NOTE:** On MX Series routers only, you can configure either Layer 3 or Layer 4 load balancing, or both at the same time.

---



**NOTE:** On I chip platforms, an unknown Layer 4 header is excluded from load-balance hashing to avoid undesired packet reordering.

---

**source-mac**—Include the source-address MAC information in the hash key.

**symmetric-hash** (MX Series routers only)—Configure the symmetric hash or symmetric hash complement for configuring symmetrical load balancing on an 802.3ad Link Aggregation Group.

- **complement** —Include the complement of the symmetric hash in the hash key.

**Required Privilege  
Level**

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

- Related Documentation**
- [Configuring Load Balancing Based on MAC Addresses](#)
  - [Configuring VPLS Load Balancing Based on IP and MPLS Information on page 897](#)
  - [Configuring VPLS Load Balancing on MX Series 3D Universal Edge Routers on page 898](#)
  - [Configuring VPLS Load Balancing on page 895](#)

## fast-aps-switch

|                            |                                                                                                                                                                                          |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | fast-aps-switch;                                                                                                                                                                         |
| <b>Hierarchy Level</b>     | [edit interfaces <i>interface-name</i> sonet-options aps]                                                                                                                                |
| <b>Release Information</b> | Statement introduced in Junos OS Release 12.1.                                                                                                                                           |
| <b>Description</b>         | (M320 routers with Channelized OC3/STM1 Circuit Emulation PIC with SFP only and EX Series switches) Reduce the Automatic Protection Switching (APS) switchover time in Layer 2 circuits. |




### NOTE:

- Configuring this statement reduces the APS switchover time only when the Layer 2 circuit encapsulation type for the interface receiving traffic from a Layer 2 circuit neighbor is SAToP.
- When the fast-aps-switch statement is configured in revertive APS mode, you must configure an appropriate value for revert time to achieve reduction in APS switchover time.
- To prevent the logical interfaces in the data path from being shut down, configure appropriate hold-time values on all the interfaces in the data path that support TDM.
- The fast-aps-switch statement cannot be configured when the APS annex-b option is configured.
- The interfaces that have the fast-aps-switch statement configured cannot be used in virtual private LAN service (VPLS) environments.

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | • <a href="#">Reducing APS Switchover Time in Layer 2 Circuits on page 395</a>                                          |

## fast-reroute-priority

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | fast-reroute-priority (high   low   medium);                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit forwarding-options]<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options],<br>[edit routing-instances <i>routing-instance-name</i> forwarding-options]                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.5.<br>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Specify the fast reroute priority for a VPLS routing instance. You can configure <b>high</b> , <b>medium</b> , or <b>low</b> fast reroute priority to prioritize specific VPLS routing instances for faster convergence and traffic restoration. Because the router repairs next hops for high-priority VPLS routing instances first, the traffic traversing a VPLS routing instance configured with <b>high</b> fast reroute priority is restored faster than the traffic for VPLS routing instances configured with <b>medium</b> or <b>low</b> fast reroute priority.                                                                                                                        |
|                                 | <div> <b>NOTE:</b> In the VPLS documentation, the word <i>router</i> in terms such as <i>PE router</i> is used to refer to any device that provides routing functions.</div>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Default</b>                  | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | <b>high</b> —Set the fast reroute priority for a VPLS routing instance to high. During a fast reroute event, the router repairs next hops for high-priority VPLS routing instances first.<br><br><b>low</b> —Set the fast reroute priority for a VPLS routing instance to low, which is the default. During a fast reroute event, the router repairs next hops for low-priority VPLS routing instances last.<br><br><b>medium</b> —Set the fast reroute priority for a VPLS routing instance to medium. During a fast reroute event, the router repairs next hops for medium-priority VPLS instances after high-priority VPLS routing instances but before low-priority VPLS routing instances. |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring VPLS Fast Reroute Priority on page 577</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## flow-label-receive-static

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | flow-label-receive-static;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit protocols l2circuit neighbor <i>neighbor-id</i> interface <i>interface-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 14.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | <p>Configure the FEC 128 VPWS pseudowire to statically push the flow label on the pseudowire packets sent to the remote egress provider edge (PE) router. The ingress PE router inserts the flow label in the pseudowire packet, irrespective of the information exchanged in the signaling plane. If the egress PE router cannot handle the pseudowire packet marked with the flow label, the packet is dropped.</p> <p>Flow-aware transport of pseudowires (FAT) flow labels enable load-balancing of MPLS packets across equal-cost multipath (ECMP) paths or link aggregation groups (LAGs) without the need for deep packet inspection of the payload. FAT flow labels can be used for LDP-signaled forwarding equivalence class (FEC) 128 and FEC 129 pseudowires for virtual private LAN service (VPLS) and virtual private wire service (VPWS) networks.</p> |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the FAT Flow Label for FEC 128 VPWS Pseudowires for Load-Balancing MPLS Traffic on page 534</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## flow-label-transmit-static

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | flow-label-transmit-static;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit protocols l2circuit neighbor <i>neighbor-id</i> interface <i>interface-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 14.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | <p>Configure the router to statically pop the flow label on the pseudowire packets received from the remote egress provider (PE) router. If the incoming pseudowire packet is not marked with the flow label, the packet is dropped by the egress PE router.</p> <p>Flow-aware transport of pseudowires (FAT) flow labels enable load-balancing of MPLS packets across equal-cost multipath (ECMP) paths or link aggregation groups (LAGs) without the need for deep packet inspection of the payload. FAT flow labels can be used for LDP-signaled forwarding equivalence class (FEC) 128 and FEC 129 pseudowires for virtual private LAN service (VPLS) and virtual private wire service (VPWS) networks.</p> |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the FAT Flow Label for FEC 128 VPWS Pseudowires for Load-Balancing MPLS Traffic on page 534</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## hot-standby

---

|                                 |                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | hot-standby;                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i> ]                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 14.2.                                                                                                                                |
| <b>Description</b>              | Turn on the protector behavior for the site. This keeps backup pseudowire in continuous standby mode and ready for traffic forwarding.                                        |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Example: Configuring MPLS Egress Protection Service Mirroring for BGP Signaled Layer 2 Services on page 471</a></li></ul> |

## hot-standby (Protocols Layer 2 Circuit)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | hot-standby;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | <p>[edit logical-systems <i>logical-system-name</i> protocols l2circuit local-switching interface <i>interface-name</i> end-interface interface <i>interface-name</i> backup-neighbor <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> backup-neighbor <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i> backup-neighbor <i>address</i>],</p> <p>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> backup-neighbor <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i> backup-neighbor <i>address</i>]</p> |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Hierarchy levels associated with the <b>backup-neighbor</b> statement added in Junos OS Release 9.2.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | <p>Configure the pseudowire to the specified backup neighbor as the hot-standby. When you configure this statement, traffic flows over both the active and hot-standby pseudowires to the backup device (either a CE device or PE router). The backup device drops the traffic from the hot-standby pseudowire, unless the active pseudowire fails. If the active pseudowire fails, the backup device automatically switches to the hot-standby pseudowire.</p> <p>Configure the <b>hot-standby</b> statement on routers that have both active and standby virtual circuits. Generally, these are access routers. On provider edge routers, configure the <b>hot-standby-vc-on'</b> statement to indicate that a hot-standby pseudowire is desired upon arrival of a PW_FWD_STDBY status-TLV.</p>                           |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Layer 2 Circuits over Both RSVP and LDP LSPs on page 355</a></li> <li>• <a href="#">Configuring Pseudowire Redundancy on the PE Router on page 180</a></li> <li>• <a href="#">Example: Configuring Layer 2 Circuit Switching Protection on page 420</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



## hot-standby-vc-on (Protocols Layer 2 Circuit)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | hot-standby-vc-on;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>neighbor-id</i> interface <i>interface-name</i> pseudowire-status-tlv],<br>[edit protocols l2circuit neighbor <i>neighbor-id</i> interface <i>interface-name</i> pseudowire-status-tlv]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | <p>On provider edge (PE) aggregation routers, configure the <b>hot-standby-vc-on</b> statement to indicate that a hot-standby pseudowire is desired upon arrival of a PW_FWD_STDBY status-tlv. This flag indicates the standby state. Configure the <b>hot-standby</b> statement on routers that have both active and standby virtual circuits. Generally, these are access routers.</p> <p>The goal of the <b>hot-standby</b> statement is to reduce the amount of traffic being discarded during primary-to-backup transition periods. This statement enables the possibility of keeping both the active and standby paths open within the Layer 2 domain. By having both the active and standby VCs able to send and receive traffic, traffic loops could potentially occur within the Layer 2 domain. In consequence, Layer 2 VCs are kept open only in the PE-to-access direction. In other words, aggregation PE devices can send traffic toward access devices, but access devices send traffic exclusively through the active VC.</p> <p>In this regard, the <b>hot-standby</b> statement is quite similar to the <b>standby</b> statement. The <b>hot-standby</b> statement allows for a faster forwarding-path switchover during transition periods, as compared to what is allowed by the <b>standby</b> statement.</p> |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Example: Configuring Pseudowire Redundancy in a Mobile Backhaul Scenario on page 371</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



## identifier (VPLS Multihoming for FEC 129)

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <code>identifier <i>identifier</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | [edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls multi-homing site <i>site-name</i> ],<br>[edit routing-instances <i>instance-name</i> protocols vpls multi-homing site <i>site-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Configure a Layer 2 VPN or VPLS multihoming identifier (MHID). An identifier needs to be configured for each multihomed site. Multihoming site identifiers are specific to a VPLS domain. They need not be unique on a provider edge (PE) router when multiple VPLS instances are present. The network layer reachability information (NLRI) advertisements sent to a CE device are identified as candidates for designated forwarder selection because the advertisements have the same multihoming identifier. Thus, you should assign the same identifier on all VPLS PE routers that are multihomed to the same customer site. |
| <div>  <p><b>NOTE:</b> The route distinguisher must be unique among PE routers participating in a multihomed site, so that the RD:MHID combination is unique across multiple VPLS domains. For example, one PE router might have a route distinguisher of 1.1.1.4:1, and another PE router in the same site might have a route distinguisher of 1.1.1.2:1. The first number can be, for example, the loopback interface address that identifies the PE router. The second number is the multihoming identifier.</p> </div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <div>  <p><b>NOTE:</b> In the VPLS documentation, the word <i>router</i> in terms such as <i>PE router</i> is used to refer to any device that provides routing functions.</p> </div>                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <i>identifier</i> —Number that identifies the multihomed site.<br><b>Range:</b> 1 through 65535                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring VPLS Multihoming (FEC 129) on page 767</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## ignore-encapsulation-mismatch

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | ignore-encapsulation-mismatch;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>          | <p>[edit logical-systems <i>logical-system-name</i> protocols l2circuit local-switching interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i>],</p> <p>[edit protocols l2circuit local-switching interface <i>interface-name</i>],</p> <p>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols evpn interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i>]</p> |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.2.</p> <p>Statement extended to support local switching in Junos OS Release 10.4.</p> <p>Statement introduced for EVPNs in Junos OS Release 13.2 for MX 3D Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Allow a Layer 2 circuit, VPLS, or EVPN to be established even though the encapsulation configured on the CE device interface does not match the encapsulation configured on the Layer 2 circuit, VPLS, or EVPN interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring EVPN Routing Instances on page 239</a></li><li>• <a href="#">Enabling the Layer 2 Circuit When the Encapsulation Does Not Match on page 353</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## ignore-mtu-mismatch

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | ignore-mtu-mismatch;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | <p>[edit logical-systems <i>logical-system-name</i> protocols l2circuit local-switching interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls],</p> <p>[edit protocols l2circuit local-switching interface <i>interface-name</i>],</p> <p>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls]</p> |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 8.5.</p> <p>Support for remote PE routers added in Junos OS Release 9.2.</p> <p>Support for Layer 2 VPNs and VPLS added in Junos OS Release 10.4.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | Ignore the MTU configuration set for the physical interface associated with the local switching interface or with the remote PE router. This allows a pseudowire to be brought up between two logical interfaces that are defined on physical interfaces with different MTU values.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Enabling Local Interface Switching When the MTU Does Not Match on page 349</a></li> <li>• <a href="#">Configuring the MTU for Layer 2 Interfaces on page 165</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## interface (EVPN Routing Instances)

---

|                                 |                                                                                                                                                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>interface <i>interface-name</i> {<br/>    ignore-encapsulation-mismatch;<br/>    interface-mac-limit <i>limit</i> {<br/>        packet-action drop;<br/>    }<br/>    no-mac-learning;<br/>    static-mac <i>mac-address</i>;<br/>}</pre>                     |
| <b>Hierarchy Level</b>          | [edit routing-instances <i>routing-instance-name</i> protocols evpn]                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2 for EVPNs on MX 3D Series routers.<br>Statement introduced in Junos OS Release 14.2 on EX Series switches.                                                                                                           |
| <b>Description</b>              | Specify each interface over which the Ethernet VPN (EVPN) traffic travels between the PE device and customer edge (CE) device. The interfaces are bound to the EVPN routing instance.                                                                              |
| <b>Options</b>                  | <p><i>interface-name</i>—Name of the interface.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                      |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring EVPN Routing Instances on page 239</a></li><li>• <i>Configuring EVPN Routing Instances on EX9200 Switches</i></li><li>• <i>evpn</i></li><li>• <a href="#">instance-type on page 1044</a></li></ul> |

## interface (Protocols Layer 2 Circuit)

**Syntax** interface *interface-name* {  
     **backup-neighbor** *address*;  
     **bandwidth** (*bandwidth* | *ctnumber bandwidth*);  
     **community** *community-name*;  
     **connection-protection**;  
     (**control-word** | **no-control-word**);  
     **description** *text*;  
     **egress-protection**;  
     **encapsulation-type** *type*;  
     **flow-label-receive**;  
     **flow-label-receive-static**;  
     **flow-label-transmit**;  
     **flow-label-transmit-static**;  
     **ignore-encapsulation-mismatch**;  
     **ignore-mtu-mismatch**;  
     **mtu** *mtu-number*;  
     **no-revert**;  
     **oam**;  
     **protect-interface** *interface-name*;  
     **pseudowire-status-tlv** **hot-standby-vc-on**;  
     **psn-tunnel-endpoint** *address*;  
     **revert-time** *seconds*;  
     **static** {  
         **switchover-delay** *milliseconds*;  
         **virtual-circuit-id** *identifier*;  
     }  
 }

**Hierarchy Level** [edit logical-systems *logical-system-name* protocols l2circuit local-switching],  
 [edit logical-systems *logical-system-name* protocols l2circuit neighbor *address*],  
 [edit protocols l2circuit local-switching],  
 [edit protocols l2circuit neighbor *address*]

**Release Information** Statement introduced before Junos OS Release 7.4.  
**flow-label-receive-static** and **flow-label-transmit-static** options introduced in Junos OS Release 14.1.

**Description** Interface over which Layer 2 circuit traffic travels.

**Options** *interface-name*—Name of the interface to configure.



**NOTE:** The commit operation fails, if the same logical interface is configured for both layer 2 circuit and ccc connection.

**connection-protection**—Enable end-to-end protection through OAM failure detection.

**flow-label-receive**—Advertise capability to pop flow label in receive direction to the remote provider edge (PE) device.

**flow-label-receive-static**—Pop flow label on the pseudowire packets received from the remote PE device. The ingress PE inserts the flow label in the pseudowire packet, irrespective of the information exchanged in the signaling plane. If the egress PE cannot handle the pseudowire packet marked with the flow label, the packet is dropped.

**flow-label-transmit**—Advertise capability to push flow label in transmit direction to the remote PE device.

**flow-label-transmit-static**—Push flow label on the pseudowire packets sent to the remote PE device. If the incoming pseudowire packet is not marked with the flow label, the packet is dropped by the egress PE.

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**

- [Configuring the Neighbor Interface for the Layer 2 Circuit on page 350](#)

---

## interface (Protocols Layer 2 VPN)

---

**Syntax**

```
interface interface-name {
 description text;
 remote-site-id remote-site-id;
}
```

**Hierarchy Level** [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols l2vpn],  
[edit routing-instances *routing-instance-name* protocols l2vpn]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Configure an interface to handle traffic for a circuit configured for the Layer 2 VPN.

**Options** *interface-name*—Name of the interface used for the Layer 2 VPN.

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**

- [Configuring the Site on page 127](#)
- [Configuring the Remote Site ID on page 128](#)

## interface (VPLS Multihoming for FEC 129)

---

|                                 |                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | interface <i>interface-name</i> {<br><b>preference</b> <i>preference-value</i> ;<br>}                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls multi-homing site <i>site-name</i> ],<br>[edit routing-instances <i>instance-name</i> protocols vpls multi-homing site <i>site-name</i> ] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                   |
| <b>Description</b>              | Configure the interface that connects this site to the VPN.<br><br>The remaining statement is explained separately.                                                                                                                              |
| <b>Options</b>                  | <i>interface-name</i> —Name of the interface (for example, <b>ge-0/1/0.1</b> ).                                                                                                                                                                  |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring VPLS Multihoming (FEC 129) on page 767</a></li> </ul>                                                                                                                  |

## interface (VPLS Routing Instances)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>interface <i>interface-name</i> {<br/>    <b>interface-mac-limit</b> <i>limit</i>;<br/>}</code>                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i> ] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b>              | Configure the interface for a pseudowire to the VPLS customer site. To complete the configuration of interfaces for a VPLS routing instance, you must also configure the interfaces specified for a VPLS site at the <b>[edit routing-instances <i>routing-instance-name</i>]</b> hierarchy level as described in <a href="#">“Configuring Routing Instances on PE Routers in VPNs” on page 9</a> .                                 |
| <b>Options</b>                  | <b><i>interface-name</i></b> —Specify the name of the interface used by the VPLS site.<br><br>The remaining statement is explained separately.                                                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the VPLS Site Interfaces on page 568</a></li><li>• <a href="#">Configuring Routing Instances on PE Routers in VPNs on page 9</a></li><li>• <a href="#">interface (Routing Instances) on page 1046</a></li></ul>                                                                                                                                                     |



## interface-mac-limit (VPLS)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>interface-mac-limit <i>limit</i> {     packet-action drop; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i> interfaces <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols evpn],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols evpn interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i> interfaces <i>interface-name</i>]</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Support for EVPNs introduced in Junos OS Release 13.2 on MX 3D Series routers.</p> <p>Support for EVPNs introduced in Junos OS Release 14.2 on EX Series switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | <p>Specify the maximum number of media access control (MAC) addresses that can be learned by the EVPN or VPLS routing instance. You can configure the same limit for all interfaces configured for a routing instance. You can also configure a limit for a specific interface.</p> <p>Starting with Junos OS Release 12.3R4, if you do not configure the parameter to limit the number of MAC addresses to be learned by a VPLS instance, the default value is not effective. Instead, if you do not include the <b>interface-mac-limit</b> option at the [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i> interfaces <i>interface-name</i>], hierarchy level, this setting is not present in the configuration with the default value of 1024 addresses. If you upgrade a router running a Junos OS release earlier than Release 12.3R4 to Release 12.3R4 or later, you must configure the <b>interface-mac-limit</b> option with a valid value for it to be saved in the configuration.</p> |
| <b>Options</b>                  | <p><b>limit</b>—Number of MAC addresses that can be learned from each interface.</p> <p><b>Range:</b> 16 through 65,536 MAC addresses</p> <p><b>Default:</b> 1024 addresses</p> <p>The remaining statement is explained separately.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring EVPN Routing Instances on page 239</a></li> <li>• <a href="#">Configuring EVPN Routing Instances on EX9200 Switches</a></li> <li>• <a href="#">Limiting the Number of MAC Addresses Learned from an Interface on page 574</a></li> <li>• <a href="#">interface on page 1120</a></li> <li>• <a href="#">mac-table-size on page 1143</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## install-nexthop

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>install-nexthop (except   lsp <i>lsp-name</i>   lsp-regex <i>lsp-regular-expression</i>);</code>                                                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> policy-options policy-statement <i>policy-name</i> term <i>term-name</i> then],<br>[edit policy-options policy-statement <i>policy-name</i> term <i>term-name</i> then]                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | Select a specific label-switched path (LSP), or select an LSP from a set of similarly named LSPs as the traffic destination for the configured community. Also can prevent the installation of any matching next hops.                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <p><b>except</b>—Prevent the installation of any matching next hops.</p> <p><b>lsp <i>lsp-name</i></b>—Configure a specific LSP.</p> <p><b>lsp-regex <i>lsp-regular-expression</i></b>—Configure a range of similarly named LSPs. You can use the following wildcard characters when configuring an LSP regular expression:</p> <ul style="list-style-type: none"><li>• Asterisk (*)—Match any characters.</li><li>• Period (.)—Match any single digit.</li></ul> |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Policy Statement for the Layer 2 Circuit Community on page 358</a></li></ul>                                                                                                                                                                                                                                                                                                                  |

## l2circuit

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> l2circuit {   local-switching {     interface interface-name {       description text;     end-interface {       interface interface-name;       protect-interface interface-name;     }     ignore-mtu-mismatch;     protect-interface interface-name;   } } neighbor address {   interface interface-name {     backup-neighbor address;     bandwidth (bandwidth   ctnumber bandwidth);     community community-name;     connection-protection;     (control-word   no-control-word);     description text;     egress-protection;     encapsulation-type type;     ignore-encapsulation-mismatch;     ignore-mtu-mismatch;     mtu mtu-number;     protect-interface interface-name;     pseudowire-status-tlv hot-standby-vc-on;     psn-tunnel-endpoint address;     virtual-circuit-id identifier;   } } traceoptions {   file filename &lt;files number&gt; &lt;size size&gt; &lt;world-readable   no-world-readable&gt;;   flag flag &lt;flag-modifier&gt; &lt;disable&gt;; } </pre> |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols],<br>[edit protocols]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 11.1 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D10 for the QFX Series and for EX4600 switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | Enables a Layer 2 circuit.<br><br>The remaining statements are explained separately.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

- Related Documentation**
- [Configuring ATM Trunking on Layer 2 Circuits on page 361](#)
  - [Configuring Bandwidth Allocation and Call Admission Control in Layer 2 Circuits on page 365](#)
  - [Configuring Interfaces for Layer 2 Circuits on page 350](#)
  - [Configuring LDP for Layer 2 Circuits on page 360](#)
  - [Configuring Policies for Layer 2 Circuits on page 357](#)
  - [Configuring Static Layer 2 Circuits on page 347](#)
  - [Tracing Layer 2 Circuit Operations on page 443](#)

---

## l2ckt

---

|                                 |                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>l2ckt {<br/>    l2vpn;<br/>    l3vpn;<br/>    labeled-bgp;<br/>    no-l2vpn;<br/>}</pre>                                                                                                        |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-options forwarding-table chained-composite-next-hop ingress],<br>[edit routing-options forwarding-table chained-composite-next-hop ingress] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.3.                                                                                                                                                       |
| <b>Description</b>              | Enable composite chained next hop for ingress Layer 2 circuit label-switched paths (LSPs).<br><br>The remaining statements are explained separately.                                                 |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                  |
| <b>Related Documentation</b>    | •                                                                                                                                                                                                    |

## l2vpn

```

Syntax l2vpn {
 (control-word | no-control-word);
 encapsulation-type type;
 oam {
 bfd-liveness-detection {
 detection-time {
 threshold milliseconds;
 }
 minimum-interval milliseconds;
 minimum-receive-interval milliseconds;
 multiplier number;
 no-adaptation;
 transmit-interval {
 threshold milliseconds;
 minimum-interval milliseconds;
 }
 version (1 | automatic);
 }
 ping-interval seconds;
 }
 site site-name {
 community COMM;
 control-word ;
 encapsulation-type ethernet;
 ignore-encapsulation-mismatch;
 ignore-mtu-mismatch;
 interface interface-name {
 description text;
 community COMM;
 control-word ;
 encapsulation-type ethernet;
 ignore-encapsulation-mismatch;
 ignore-mtu-mismatch;
 mtu 1500;
 no-control-word;
 oam {
 bfd-liveness-detection {
 detection-time {
 threshold milliseconds;
 }
 }
 minimum-interval milliseconds;
 minimum-receive-interval milliseconds;
 multiplier number;
 no-adaptation;
 transmit-interval {
 threshold milliseconds;
 minimum-interval milliseconds;
 }
 version (1 | automatic);
 }
 ping-interval seconds; seconds;
 }
 }
}

```

```

 remote-site-id remote-site-id;
 target-attachment-identifier identifier;
}
mtu 1500;
no-control-word;
oam {
 bfd-liveness-detection {
 detection-time {
 threshold milliseconds;
 }
 minimum-interval milliseconds;
 minimum-receive-interval milliseconds;
 multiplier number;
 no-adaptation;
 transmit-interval {
 threshold milliseconds;
 minimum-interval milliseconds;
 }
 version (1 | automatic);
 }
 ping-interval seconds; seconds;
}
site-identifier identifier;
site-preference preference-value {
 backup;
 primary;
}
source-attachment-identifier identifier;
}
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> routing-instances <i>routing-instance-name</i> protocols],<br>[edit routing-instances <i>routing-instance-name</i> protocols]                          |
| Release Information      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 11.1 for EX Series switches.                                                                              |
| Description              | Enable a Layer 2 VPN routing instance on a PE router or switch.<br><br>The remaining statements are explained separately.                                                                               |
| Required Privilege Level | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                     |
| Related Documentation    | <ul style="list-style-type: none"> <li><a href="#">Configuring a Layer 2 VPN Routing Instance on page 127</a></li> <li><a href="#">Configuring an MPLS-Based Layer 2 VPN (CLI Procedure)</a></li> </ul> |

## l2vpn (routing-options)

---

|                                 |                                                                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>l2vpn {   l2ckt;   l3vpn;   labeled-bgp;   no-l2ckt; }</pre>                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-options forwarding-table<br>chained-composite-next-hop ingress],<br>[edit routing-options forwarding-table chained-composite-next-hop ingress] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.3.                                                                                                                                                          |
| <b>Description</b>              | <p>Enable composite chained next hop for ingress Layer 2 virtual private network (VPN) label-switched paths (LSPs).</p> <p>The remaining statements are explained separately.</p>                       |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>•</li> </ul>                                                                                                                                                     |

## l2vpn-id

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>l2vpn-id (as-number:id   ip-address:id);</code>                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> ],<br>[edit routing-instances <i>instance-name</i> ]                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.4R2.                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | Specify a globally unique Layer 2 VPN community identifier for the instance.                                                                                                                                                                                                                                                                                                                         |
| <b>Options</b>                  | <p><i>as-number:id</i>—Autonomous system number (<i>l2vpn-id:as-number:2-byte-number</i>. For example: <i>l2vpn-id l2vpn-id:100:200</i>. The AS number can be in the range from 1 through 65,535.</p> <p><i>ip-address:id</i>—IP address (<i>l2vpn-id:ip-address:2-byte-number</i>. For example: <i>l2vpn-id l2vpn-id:10.1.1.1:2</i>. The IP address can be any globally unique unicast address.</p> |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Example: Configuring BGP Autodiscovery for LDP VPLS on page 725</a></li><li>• <a href="#">Example: Configuring BGP Autodiscovery for LDP VPLS with User-Defined Mesh Groups on page 742</a></li><li>• <a href="#">Example: Configuring FEC 129 BGP Autodiscovery for VPWS on page 708</a></li></ul>                                              |



## l2vpn-use-bgp-rules

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | l2vpn-use-bgp-rules;                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols bgp path-selection],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp path-selection],<br>[edit protocols bgp path-selection],<br>[edit routing-instances <i>routing-instance-name</i> protocols bgp path-selection]                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.<br>Statement introduced in Junos OS Release 12.3 for ACX Series routers.                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | Enable routers to use both the BGP path selection algorithm and the designated forwarder path selection algorithm when selecting the preferred path to each destination in a Layer 2 VPN or VPLS routing instance. The BGP path selection algorithm is used by all of the Provider routers participating in the routing instance. The designated forwarder path selection algorithm is used by the PE router participating in the routing instance. |
| <b>Default</b>                  | By default, the designated forwarder path selection algorithm is used to select the best path to reach each destination within Layer 2 VPN and VPLS routing instances.                                                                                                                                                                                                                                                                              |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Enabling BGP Path Selection for Layer 2 VPNs and VPLS on page 173</a></li> <li>• <a href="#">route-distinguisher on page 1051</a></li> </ul>                                                                                                                                                                                                                                                   |

## label-allocation

|                                 |                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | label-allocation per-instance;                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit routing-instances <i>routing-instance-name</i> protocols evpn]                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2 on MX 3D Series routers.<br>Statement introduced in Junos OS Release 14.2 on EX Series switches. |
| <b>Description</b>              | Specifies the MPLS label allocation setting for the EVPN routing instance.                                                                     |
| <b>Options</b>                  | <b>per-instance</b> —Allocates a single MPLS label for the EVPN routing instance.                                                              |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring EVPN Routing Instances on page 239</a></li> </ul>                             |

## label-block-size

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | label-block-size <i>size</i> ;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>profile-name</i> routing-instances <i>instance-name</i> protocols vpls],<br>[edit routing-instances <i>instance-name</i> protocols vpls]                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>              | Configure the label block size for VPLS labels.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Default</b>                  | 8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <ul style="list-style-type: none"><li>• 2—Allocate the label blocks in increments of 2. For a VPLS domain that has only two sites with no future expansion plans.</li><li>• 4—Allocate the label blocks in increments of 4.</li><li>• 8 (default)—Allocate the label blocks in increments of 8.</li><li>• 16—Allocate the label blocks in increments of 16. A label block size of 16 enables you to minimize the number of routes in the VPLS domain. Use this setting only if the number of routes is the most important concern.</li></ul> |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Label Block Size for VPLS on page 596</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                      |

## label-switched-path-template (Multicast)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>label-switched-path-template {   (default-template   <i>lsp-template-name</i>); }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | <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> |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>              | <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 <b>label-switched-path-template</b> statement, so you must configure either the default-template using the <b>default-template</b> option, or you must specify the name of your preconfigured LSP template.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                  | <p><b>default-template</b>—Specify that the default LSP template be used for the dynamically generated LSPs.</p> <p><b><i>lsp-template-name</i></b>—Specify the name of an LSP to be used as a template for the dynamically generated LSPs.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring Ingress Replication for IP Multicast Using MBGP MVPNs on page 851</a></li> <li>• <a href="#">Configuring Point-to-Multipoint LSPs for an MBGP MVPN</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

- [Configuring Dynamic Point-to-Multipoint Flooding LSPs on page 850](#)
- [Configuring RSVP Automatic Mesh](#)

## local-switching (Layer 2 Circuits)

---

**Syntax**    local-switching {  
              interface *interface-name* {  
                  description *text*;  
                  encapsulation-type;  
                  end-interface {  
                      interface *interface-name*;  
                      no-revert;  
                      protect-interface *interface-name*;  
                  }  
                  ignore-encapsulation-mismatch;  
                  ignore-mtu-mismatch;  
                  no-revert;  
                  protect-interface *interface-name*;  
              }  
          }

**Hierarchy Level**    [edit logical-systems *logical-system-name* protocols l2circuit],  
                          [edit protocols l2circuit]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Configure a local switching interface. A local switching interface allows you to terminate a virtual circuit on the local router.

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**    • [Configuring Local Interface Switching in Layer 2 Circuits on page 348](#)

## local-switching (VPLS)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | local-switching;                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> ]                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.3.                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>              | Allows you to terminate multiple Layer 2 circuit pseudowires at a single VPLS mesh group. Note that when using <a href="#">vpls-id-list</a> , you can enable local-switching to allow local switching of traffic (including BUM traffic) between multiple pseudo wires. Enabling local-switching also eliminates the need to have a dedicated mesh-group for each LDP spoke pseudo wire (which has a limit of 14). |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Switching Between Pseudowires Using VPLS Mesh Groups on page 558</a></li> </ul>                                                                                                                                                                                                                                                                   |

## mac-flush

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>mac-flush [ <i>explicit-mac-flush-message-options</i> ];</code>                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>     | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> ] |
| <b>Release Information</b> | Statement introduced in Junos OS Release 10.0.                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>         | Enable media access control (MAC) flush processing for the virtual private LAN service (VPLS) routing instance or for the mesh group under a VPLS routing instance. MAC flush processing removes MAC addresses from the MAC address database that have been learned dynamically. With the dynamically learned MAC addresses removed, MAC address convergence requires less time to complete.                                                                |

For certain cases where MAC flush processing is not initiated by default, you can also specify *explicit-mac-flush-message-options* that additionally configure the router to send explicit MAC flush messages. To configure the router to send explicit MAC flush messages under specific conditions, include *explicit-mac-flush-message-options* with the statement.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

In certain cases, BGP updates sent by the provider edge (PE) device are delayed for 1 to 5 seconds.

This happens when all of the following conditions are true:

- BGP-based VPLS multihoming sites are configured.
- The **mac-flush** statement is included in the configuration.
- a non-minimum designated-forwarder site (site-x, for example) transitions to non-designated-forwarder status

The BGP update being delayed corresponds to the explicit-MAC flush notification message sent by site-x's PE device (PE2, for example). This BGP update message is not deferred if the designated-forwarder status is lost due to a locally-triggered event (for example, a local attachment-circuit interface going down). In other words, BGP update messages are deferred (in Device PE2) only when the designated-forwarder state is lost due to external events taking place in remote PE devices that also hold site-x (for example, in PE1). Suppose, for example, that Device PE1 is the default designated-forwarder with site-x's local interface in the DOWN state. Device PE2 defers BGP update message after Device PE1's local interface comes back to the UP state.

**Options** *explicit-mac-flush-message-options*—(Optional) You can specify one or more of the following explicit MAC flush message options:

- **any-interface**—(Optional) Send a MAC flush message when any customer-facing attachment circuit interface goes down.
- **any-spoke**—(Optional) Send a MAC FLUSH-FROM-ME flush message to all provider edge (PE) routers in the core when one of the spoke pseudowires between the multitenant unit switch and the other network-facing provider edge (NPE) router goes down, causing the multitenant unit switch to switch to this NPE router.



**NOTE:** This option has a similar effect in a VPLS multihoming environment with multiple multitenant unit switches connected to NPE routers, where both multitenant unit switches have pseudowires that terminate in a mesh group with local-switching configured. If the **any-spoke** option is enabled, then both PE routers send MAC FLUSH-FROM-ME flush messages to all PEs in the core.

- **propagate**—(Optional) Propagate MAC flush to the core.

**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring VPLS Routing Instances on page 563](#)
- [Configuring Interoperability Between BGP Signaling and LDP Signaling in VPLS on page 556](#)

## mac-statistics

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | mac-statistics;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | <p>[edit bridge-domains <i>bridge-domain-name</i> bridge-options],</p> <p>[edit logical-systems <i>logical-system-name</i> bridge-domains <i>bridge-domain-name</i> bridge-options],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> bridge-options],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> switch-options],</p> <p>[edit logical-systems <i>logical-system-name</i> switch-options],</p> <p>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> bridge-options],</p> <p>[edit routing-instances <i>routing-instance-name</i> switch-options],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols evpn],</p> <p>[edit switch-options],</p> <p>[edit switch-options],</p> <p>[edit vlans <i>vlan-name</i> switch-options]</p> |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 8.4.</p> <p>Support for the <b>switch-options</b> statement added in Junos OS Release 9.2.</p> <p>Support for top-level configuration for the <b>virtual-switch</b> type of routing instance added in Junos OS Release 9.2. In Junos OS Release 9.1 and earlier, the routing instances hierarchy supported this statement only for a VPLS instance or a bridge domain configured within a virtual switch.</p> <p>Support for logical systems added in Junos OS Release 9.6.</p> <p>[edit switch-options] and [edit vlans <i>vlan-name</i> switch-options] hierarchy levels introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support for EVPNs added in Junos OS Release 13.2 for MX 3D Series routers.</p> <p>[edit switch-options] and [edit vlans <i>vlan-name</i> switch-options] hierarchy levels introduced in Junos OS Release 13.2 for the QFX Series.</p>                          |
| <b>Description</b>              | (MX Series routers, EX Series switches, and QFX Series only) For bridge domains or VLANs, enable MAC accounting either for a specific bridge domain or VLAN, or for a set of bridge domains or VLANs associated with a Layer 2 trunk port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Default</b>                  | disabled                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Understanding Layer 2 Learning and Forwarding for Bridge Domains</i></li> <li>• <i>Layer 2 Learning and Forwarding for VLANs Overview</i></li> <li>• <i>Understanding Layer 2 Learning and Forwarding for Bridge Domains Functioning as Switches with Layer 2 Trunk Ports</i></li> <li>• <i>Layer 2 Learning and Forwarding for VLANs Acting as a Switch for a Layer 2 Trunk Port</i></li> <li>• <a href="#">Configuring EVPN Routing Instances on page 239</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                     |



- *Configuring EVPN Routing Instances on EX9200 Switches*

## mac-table-aging-time

**Syntax** `mac-table-aging-time time;`

**Hierarchy Level** [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vpls],  
[edit routing-instances *routing-instance-name* protocols vpls]  
[edit bridge-options],  
[edit routing-instances *routing-instance-name* protocols evpn]



**NOTE:** For MX Series routers, the configuration statement is supported at the [bridge-options], [protocols vpls], and [protocols evpn] hierarchy levels only.

**Release Information** Statement introduced in Junos OS Release 7.4.  
Statement introduced in Junos OS Release 15.1 for MX Series routers.

**Description** Modify the timeout interval for the MAC table.

For MX Series routers, you can use the **global-mac-table-aging-time** statement at the [edit protocols l2-learning] hierarchy level to configure the timeout interval at the global level or use the **mac-table-aging-time** to configure the timeout interval for a bridge domain or for a specific VPLS or EVPN instance. If multiple timeout interval values are configured on a router, the router determines the timeout interval value in the following order of priority:

- Timeout interval configured at the VPLS or EVPN instance
- Timeout interval configured for the bridge domain
- Global timeout interval configured on the router



**NOTE:** For MX Series routers, the timeout interval configuration feature is supported on routers with MPCs only.


**Options** *time*—Specify the number of seconds to wait between MAC table clearings.  
**Range:** 10 through 1,000,000 seconds  
**Default:** 300 seconds

**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring the VPLS MAC Table Timeout Interval on page 573](#)
- [Configuring the MAC Table Timeout Interval](#)

## mac-table-size

|                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                                            | <pre>mac-table-size size {     packet-action drop; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                                                   | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls],<br>[edit routing-instances <i>routing-instance-name</i> protocols evpn],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls]                                                                                                                                                                                                            |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                                                                               | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 13.2 for EVPNs on MX 3D Series routers.<br>Statement introduced in Junos OS Release 14.2 for EX Series switches.                                                                                                                                                                                                                                                               |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                                                       | Specify the size of the MAC address table.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                                                                                                                                                                                                                                                                                                                                                           | <p><b>size</b>—Size of the MAC address table.</p> <p><b>Range:</b></p> <ul style="list-style-type: none"> <li>• (M Series and T Series routers only) 16 through 65,536 MAC addresses</li> <li>• (MX Series routers only) 16 through 1,048,575 MAC addresses</li> <li>• (T4000 routers with Type 5 FPCs only) 16 through 262,143 MAC addresses</li> </ul>                                                                                                                     |
| <div>  <p><b>NOTE:</b> Before modifying the size of the MAC address table (to 262,143 addresses), you must enable network services mode by including the <b>enhanced-mode</b> statement at the [edit chassis network-services] hierarchy level and then reboot the router.</p> </div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <p><b>Default:</b> 512 MAC addresses</p> <p>The remaining statement is explained separately.</p>                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                                                                          | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>• <a href="#">Configuring EVPN Routing Instances on page 239</a></li> <li>• <a href="#">Configuring EVPN Routing Instances on EX9200 Switches</a></li> <li>• <a href="#">Configuring the Size of the VPLS MAC Address Table on page 574</a></li> <li>• <a href="#">Configuring Improved VPLS MAC Address Learning on T4000 Routers with Type 5 FPCs on page 918</a></li> <li>• <i>enhanced-mode</i></li> <li>• <i>evpn</i></li> </ul> |

## mesh-group (Protocols VPLS)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre> mesh-group <i>mesh-group-name</i> {   l2vpn-id (<i>as-number:id</i>   <i>ip-address:id</i>);   local-switching;   mac-flush [ <i>explicit-mac-flush-message-options</i> ];   neighbor <i>address</i> {...}   peer-as all;   pseudowire-status-tlv;   route-distinguisher (<i>as-number:id</i>   <i>ip-address:id</i>);   vpls-id <i>number</i>;   vrf-export [ <i>policy-names</i> ];   vrf-import [ <i>policy-names</i> ];   vrf-target {     community;     import <i>community-name</i>;     export <i>community-name</i>;   } } </pre> |
| <b>Hierarchy Level</b>     | <pre> [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   vpls], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   vpls site <i>site-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols vpls], [edit routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i>] </pre>                                                                                                        |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 9.0.</p> <p><b>local-switching</b>, <b>mac-tlv-receive</b>, <b>mac-tlv-send</b>, and <b>peer-as</b> options introduced in Junos OS Release 9.3.</p> <p><b>pseudowire-status-tlv</b> and <b>mac-flush</b> options introduced in Junos OS Release 10.0.</p> <p><b>route-distinguisher</b>, <b>vrf-export</b>, <b>vrf-import</b>, and <b>vrf-target</b> options introduced in Junos OS Release 11.2.</p>                                                                                                |
| <b>Description</b>         | <p>Specify the virtual private LAN service (VPLS) mesh group. The statement options allow you to specify each provider edge (PE) router that is a member of the mesh group. This statement is also used in the configuration of inter-autonomous system (AS) VPLS with media access control (MAC) operations.</p>                                                                                                                                                                                                                                |



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

|                                 |                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Options</b>                  | <p><b><i>mesh-group-name</i></b>—Name of the VPLS mesh group.</p> <p>The remaining statements are explained separately.</p>    |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p> |

- Related Documentation**
- [Configuring VPLS Routing Instances on page 563](#)
  - [Configuring Interoperability Between BGP Signaling and LDP Signaling in VPLS on page 556](#)

## minimum-interval (BFD Liveness Detection)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>minimum-interval <i>milliseconds</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>     | <p>[edit logical-systems <i>logical-system-name</i> protocols bgp bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection],</p> <p>[edit protocols bgp bfd-liveness-detection],</p> <p>[edit protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit protocols bgp group <i>group-name</i> neighbor <i>address</i> bgp bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection]</p> |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 8.5.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 13.2 for Layer 2 VPN and VPLS.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>         | <p>Configure the minimum interval after which the local routing device transmits hello packets and then expects to receive a reply from a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can specify the minimum transmit and receive intervals separately using the <a href="#">minimum-interval</a> (specified under the <a href="#">transmit-interval</a> statement) and <a href="#">minimum-receive-interval</a> statements.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>             | <p><i>milliseconds</i>—Specify the minimum interval value for BFD liveliness detection.</p> <p><b>Range:</b> 1 through 255,000</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**Required Privilege** routing—To view this statement in the configuration.  
**Level** routing-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring BFD for Layer 2 VPN and VPLS on page 186](#)
- *Example: Configuring BFD for Static Routes*
- *bfd-liveness-detection*
- [minimum-receive-interval on page 1150](#)
- [transmit-interval on page 1218](#)

## minimum-interval (transmit-interval)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>minimum-interval <i>milliseconds</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>     | <p>[edit logical-systems <i>logical-system-name</i> protocols bgp bfd-liveness-detection transmit-interval],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection transmit-interval],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection transmit-interval],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection transmit-interval],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection transmit-interval],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection transmit-interval],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection transmit-interval],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection transmit-interval],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection transmit-interval],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection transmit-interval],</p> <p>[edit protocols bgp bfd-liveness-detection transmit-interval],</p> <p>[edit protocols bgp group <i>group-name</i> bfd-liveness-detection transmit-interval],</p> <p>[edit protocols bgp group <i>group-name</i> neighbor <i>address</i> bgp bfd-liveness-detection transmit-interval],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection transmit-interval],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection transmit-interval],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection transmit-interval],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection transmit-interval],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection transmit-interval],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection transmit-interval],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection transmit-interval]</p> |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 8.2.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for BFD authentication introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 13.2 for Layer 2 VPN and VPLS.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b>         | Configure the minimum interval at which the local routing device transmits hello packets to a neighbor with which it has established a BFD session. Optionally, instead of using                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



this statement at this hierarchy level, you can configure the minimum transmit interval using the [minimum-interval](#) statement at the **bfd-liveness-detection** hierarchy level.

**Options** *milliseconds*—Minimum transmit interval value.

**Range:** 1 through 255,000



**NOTE:** The threshold value specified in the **threshold** statement must be greater than the value specified in the **minimum-interval** statement for the **transmit-interval** statement.

**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring BFD for Layer 2 VPN and VPLS on page 186](#)
- [Example: Configuring BFD for Static Routes](#)
- [bfd-liveness-detection](#)
- [minimum-interval on page 1146](#)
- [threshold on page 1207](#)

## minimum-receive-interval (BFD Liveness Detection)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>minimum-receive-interval <i>milliseconds</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>     | <p>[edit logical-systems <i>logical-system-name</i> protocols bgp bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection],</p> <p>[edit protocols bgp bfd-liveness-detection],</p> <p>[edit protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit protocols bgp group <i>group-name</i> neighbor <i>address</i> bgp bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection]</p> |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 8.5.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for BFD authentication introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 13.2 for Layer 2 VPN and VPLS.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>         | Configure the minimum interval after which the local routing device must receive a reply from a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can configure the minimum receive interval using the <b>minimum-interval</b> statement.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>             | <p><b><i>milliseconds</i></b>—Specify the minimum receive interval value.</p> <p><b>Range:</b> 1 through 255,000</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|                                 |                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring BFD for Layer 2 VPN and VPLS on page 186</a></li><li>• <i>Example: Configuring BFD for Static Routes</i></li><li>• <i>bfd-liveness-detection</i></li><li>• <a href="#">minimum-interval on page 1146</a></li><li>• <a href="#">transmit-interval on page 1218</a></li></ul> |

## mtu

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>mtu bytes;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>     | <pre>[edit interfaces <i>interface-name</i>], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>], [edit interfaces <i>interface-range name</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>], [edit logical-systems <i>logical-system-name</i> protocols l2circuit local-switching interface <i>interface-name</i> backup-neighbor <i>address</i>], [edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> backup-neighbor <i>address</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls], [edit protocols l2circuit local-switching interface <i>interface-name</i> backup-neighbor <i>address</i>], [edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>] [edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> backup-neighbor <i>address</i>], [edit routing-instances <i>routing-instance-name</i> protocols l2vpn interface <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols vpls]</pre> |
| <b>Release Information</b> | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for Layer 2 VPNs and VPLS introduced in Junos OS Release 10.4.</p> <p>Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.</p> <p>Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.</p> <p>Support at the <code>[set interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>ccc</i>]</code> hierarchy level introduced in Junos OS Release 12.3R3 for MX Series routers.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b>         | <p>Specify the maximum transmission unit (MTU) size for the media or protocol. The default MTU size depends on the device type. Changing the media MTU or protocol MTU causes an interface to be deleted and added again.</p> <p>To route jumbo data packets on an integrated routing and bridging (IRB) interface or routed VLAN interface (RVI) on EX Series switches, you must configure the jumbo MTU size on the member physical interfaces of the VLAN that you have associated with the IRB interface or RVI, as well as on the IRB interface or RVI itself (the interface named <i>irb</i> or <i>vlan</i>, respectively).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |



**CAUTION:** For EX Series switches, setting or deleting the jumbo MTU size on an IRB interface or RVI while the switch is transmitting packets might cause packets to be dropped.



---

**NOTE:**

The MTU for an IRB interface is calculated by removing the Ethernet header overhead [6(DMAC)+6(SMAC)+2(EtherType)]. Because, the MTU is the lower value of the MTU configured on the IRB interface and the MTU configured on the IRB's associated bridge domain IFDs or IFLs, the IRB MTU is calculated as follows:

- In case of Layer 2 IFL configured with the `flexible-vlan-tagging` statement, the IRB MTU is calculated by including 8 bytes overhead (SVLAN+CVLAN).
  - In case of Layer 2 IFL configured with the `vlan-tagging` statement, the IRB MTU is calculated by including a single VLAN 4 bytes overhead.
-



---

**NOTE:**

- If a packet whose size is larger than the configured MTU size is received on the receiving interface, the packet is eventually dropped. The value considered for MRU (maximum receive unit) size is also the same as the MTU size configured on that interface.
- Not all devices allow you to set an MTU value, and some devices have restrictions on the range of allowable MTU values. You cannot configure an MTU for management Ethernet interfaces (fxp0, em0, or me0) or for loopback, multilink, and multicast tunnel devices.
- On ACX Series routers, you can configure the protocol MTU by including the `mtu` statement at the [edit interfaces *interface-name* unit *logical-unit-number* family inet] or [edit interfaces *interface-name* unit *logical-unit-number* family inet6] hierarchy level.
  - If you configure the protocol MTU at any of these hierarchy levels, the configured value is applied to all families that are configured on the logical interface.
  - If you are configuring the protocol MTU for both inet and inet6 families on the same logical interface, you must configure the same value for both the families. It is not recommended to configure different MTU size values for inet and inet6 families that are configured on the same logical interface.
- For IRB interfaces, MTU is calculated by removing the Ethernet header overhead ( $6(\text{DMAC}) + 6(\text{SMAC}) + 2(\text{EtherType})$ ), and the MTU is a minimum of the two values:
  - Configured MTU
  - Associated bridge domain's physical or logical interface MTU
    - For Layer 2 logical interfaces configured with flexible-vlan-tagging, IRB MTU is calculated by including 8 bytes overhead (SVLAN+CVLAN).
    - For Layer 2 logical interfaces configured with vlan-tagging, IRB MTU is calculated by including single VLAN 4 bytes overhead.



---

**NOTE:** Changing the Layer 2 logical interface option from vlan-tagging to flexible-vlan-tagging or vice versa adjusts the logical interface MTU by 4 bytes with the existing MTU size. As a result, the Layer 2 logical interface is deleted and re-added, and the IRB MTU is re-computed appropriately.

---

For more information about configuring MTU for specific interfaces and router or switch combinations, see *OBSOLETE: Configuring the Media MTU*.

**Options**    *bytes*—MTU size.

**Range:** 256 through 9192 bytes, 256 through 9216 (EX Series switch interfaces), 256 through 9500 bytes (Junos OS 12.1X48R2 for PTX Series routers)

**Default:** 1500 bytes (INET, INET6, and ISO families), 1448 bytes (MPLS), 1514 bytes (EX Series switch interfaces)

**Required Privilege**    interface—To view this statement in the configuration.  
**Level**    interface-control—To add this statement to the configuration.

**Related**    • *OBSOLETE: Configuring the Media MTU*  
**Documentation**    • [Configuring the MTU for Layer 2 Interfaces on page 165](#)  
    • *OBSOLETE-Setting the Protocol MTU*

## multiplier (BFD Liveness Detection)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>multiplier <i>number</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>     | <p>[edit logical-systems <i>logical-system-name</i> protocols bgp bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection],</p> <p>[edit protocols bgp bfd-liveness-detection],</p> <p>[edit protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit protocols bgp group <i>group-name</i> neighbor <i>address</i> bgp bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection]</p> |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 8.5.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for BFD authentication introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 13.2 for Layer 2 VPN and VPLS.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>         | Configure the number of hello packets not received by a neighbor that causes the originating interface to be declared down.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Options</b>             | <p><i>number</i>—Number of hello packets.</p> <p><b>Range:</b> 1 through 255</p> <p><b>Default:</b> 3</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |



**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring BFD for Layer 2 VPN and VPLS on page 186](#)
- *Example: Configuring BFD for Static Routes*
- *bfd-liveness-detection*

## multi-homing (VPLS Multihoming for FEC 128)

**Syntax** multi-homing;

**Hierarchy Level** [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vpls site *site-name*],  
[edit routing-instances *routing-instance-name* protocols vpls site *site-name*]

**Release Information** Statement introduced in Junos OS Release 7.5.

**Description** Specify the PE router as being a part of a multihomed site. Include this statement on all PE routers associated with a particular site. Configuration of this statement tracks BGP peers. If no BGP peer is available, all active interfaces for a site are deactivated.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Multihoming on the PE Router on page 755](#)

## multi-homing (VPLS Multihoming for FEC 129)

```
Syntax multi-homing {
 peer-active;
 site site-name {
 active-interface interface-name {
 any;
 primary interface-name;
 }
 identifier identifier;
 interface interface-name {
 preference preference-value;
 }
 peer-active;
 preference (preference-value | backup | primary);
 }
}
```

**Hierarchy Level** [edit logical-systems *logical-system-name* routing-instances *instance-name* protocols vpls],  
[edit routing-instances *instance-name* protocols vpls]

**Release Information** Statement introduced in Junos OS Release 12.3.

**Description** For VPLS autodiscovery (FEC 129), specify the parameters for multihoming to two or more provider edge (PE) routers.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

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**

- [Example: Configuring VPLS Multihoming \(FEC 129\) on page 767](#)

## neighbor (Protocols Layer 2 Circuit)

```
Syntax neighbor address {
 interface interface-name {
 backup-neighbor address {
 community name;
 hot-standby;
 psn-tunnel-endpoint address;
 standby;
 virtual-circuit-id number;
 }
 bandwidth (bandwidth | ctnumber bandwidth);
 community community-name;
 (control-word | no-control-word);
 description text;
 egress-protection {
 protected-l2circuit {
 egress-pe address;
 ingress-pe address;
 virtual-circuit-id identifier;
 }
 protector-interface interface-name;
 protector-pe address {
 context-identifier identifier;
 lsp lsp-name;
 }
 }
 }
 encapsulation-type type;
 ignore-encapsulation-mismatch;
 ignore-mtu-mismatch;
 mtu mtu-number;
 no-revert;
 protect-interface interface-name;
 pseudowire-status-tlv hot-standby-vc-on;
 psn-tunnel-endpoint address;
 revert-time seconds;
 static {
 incoming-label label;
 outgoing-label label;
 send-oam;
 }
 switchover-delay milliseconds;
 virtual-circuit-id identifier;
 }
```

**Hierarchy Level** [edit logical-systems *logical-system-name* protocols l2circuit],  
[edit protocols l2circuit]

**Release Information** Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 11.1 for EX Series switches.

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>              | Each Layer 2 circuit is represented by the logical interface connecting the local provider edge (PE) router or switch to the local customer edge (CE) router or switch. All the Layer 2 circuits using a particular remote PE router or switch designated for remote CE routers or switches are listed under the <b>neighbor</b> statement (neighbor designates the PE router or switch). Each neighbor is identified by its IP address and is usually the end-point destination for the LSP tunnel (transporting the Layer 2 circuit). |
| <b>Options</b>                  | <b>address</b> —IP address of a neighboring router or switch.<br><br>The remaining statements are explained separately.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Neighbor Interface for the Layer 2 Circuit on page 350</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                |

## neighbor (Protocols VPLS)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre> neighbor <i>neighbor-id</i> {     associate-profile {         <i>dynamic-profile-name</i>;         profile-variable-set <i>profile-variable-set-name</i>;     }     backup-neighbor {...}     community <i>community-name</i>;     connection-protection;     encapsulation-type <i>type</i>;     ignore-encapsulation-mismatch;     oam {         bfd-liveness-detection {             detection-time {                 threshold <i>milliseconds</i>;             }             minimum-interval <i>milliseconds</i>;             minimum-receive-interval <i>milliseconds</i>;             multiplier <i>number</i>;             no-adaptation;             transmit-interval {                 minimum-interval <i>milliseconds</i>;                 threshold <i>milliseconds</i>;             }             version (1   automatic);         }         ping-interval;     }     pseudowire-status-tlv;     psn-tunnel-endpoint <i>address</i>;     revert-time <i>seconds</i>;     static {         incoming-label <i>label</i>;         outgoing-label <i>label</i>;     }     switchover-delay <i>milliseconds</i>;     vpls-id-list <i>vc-id-numbers</i>; } </pre> |
| <b>Hierarchy Level</b>     | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls],</p> <p>[edit routing-instances <i>instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>]</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 8.4.</p> <p>The <b>pseudowire-status-tlv</b> option was added in Junos OS Release 10.0.</p> <p>The <b>vpls-id-list</b> option was added in Junos OS Release 14.2 for MX Series routers to provide support for multiple pseudowires between the same pair of PEs in LDP-VPLS.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>         | Specify each of the PE routers participating in the VPLS domain. Configuring this statement enables LDP for signaling VPLS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

**Options** *neighbor-id*—Specify the neighbor identifier for each PE router participating in the VPLS domain.

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**

- [Configuring LDP Signaling for VPLS on page 569](#)

## no-adaptation (BFD Liveness Detection)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | no-adaptation;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | <p>[edit logical-systems <i>logical-system-name</i> protocols bgp bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection],</p> <p>[edit protocols bgp bfd-liveness-detection],</p> <p>[edit protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit protocols bgp group <i>group-name</i> neighbor <i>address</i> bgp bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection]</p> |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.0</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for BFD authentication introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 13.2 for Layer 2 VPN and VPLS.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | Configure BFD sessions not to adapt to changing network conditions. We recommend that you <i>do not</i> disable BFD adaptation unless it is preferable to have BFD adaptation disabled in your network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

- Related Documentation**
- [Configuring BFD for Layer 2 VPN and VPLS on page 186](#)
  - *Example: Configuring BFD for Static Routes*
  - *bfd-liveness-detection*

---

## **no-control-word (BGP VPLS)**

---

|                                 |                                                                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | no-control-word;                                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls]                                                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 14.1.                                                                                                                                                                                                                |
| <b>Description</b>              | Set <b>no-control-word</b> to request that other routers <i>not</i> insert a control word between the label stack and the MPLS payload. This is the default setting for BGP VPLS.                                                                             |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Control Word for BGP VPLS Overview on page 550</a></li><li>• <a href="#">Configuring a Control Word for BGP VPLS on page 551</a></li><li>• <a href="#">control-word (BGP VPLS) on page 1084</a></li></ul> |



## no-control-word (Protocols Layer 2 VPN)

|                            |                                                                                                                                                                                                                              |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | no-control-word;                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>     | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols <a href="#">l2vpn</a> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols <a href="#">l2vpn</a> ] |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                            |
| <b>Description</b>         | Disable the control word. This might be necessary on networks with equipment that does not support the control word.                                                                                                         |



**NOTE:** The following configuration statements are ignored for time-division multiplexing pseudowires at the [edit protocols [l2vpn](#)] hierarchy level:

- control-word
- no-control-word

|                                 |                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>                  | The control word is enabled by default. Use the <b>no-control-word</b> statement to disable the control word.                                                                    |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Disabling the Control Word for Layer 2 VPNs on page 167</a></li> <li>• <a href="#">control-word on page 1083</a></li> </ul> |

## no-l2ckt

---

|                            |                                                                                                                                                                                                      |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | no-l2ckt;                                                                                                                                                                                            |
| <b>Hierarchy Level</b>     | [edit logical-systems <i>logical-system-name</i> routing-options forwarding-table chained-composite-next-hop ingress],<br>[edit routing-options forwarding-table chained-composite-next-hop ingress] |
| <b>Release Information</b> | Statement introduced in Junos OS Release 13.3.                                                                                                                                                       |
| <b>Description</b>         | Disable composite chained next hop for ingress Layer 2 circuit label-switched paths (LSPs).<br><br>The remaining statements are explained separately.                                                |



**NOTE:** For PTX Series routers, it is recommended that you do not use this command and disable composite chained next hop for ingress LSPs.


|                                 |                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration. |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------|

## no-l2vpn

---

|                                 |                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | no-l2vpn {<br>l2ckt;<br>l3vpn;<br>labeled-bgp;<br>no-l2ckt;<br>}                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-options forwarding-table chained-composite-next-hop ingress],<br>[edit routing-options forwarding-table chained-composite-next-hop ingress] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.3.                                                                                                                                                       |
| <b>Description</b>              | Disable composite chained next hop for ingress Layer 2 virtual private network (VPN) label-switched paths (LSPs).<br><br>The remaining statements are explained separately.                          |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                  |

## no-local-switching (VPLS)

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | no-local-switching;                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | [edit bridge-domains <i>bridge-domain-name</i> ]                                                                                                                                                                                |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Statement introduced in Junos OS Release 8.5.                                                                                                                                                                                   |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Prevent CE devices from communicating directly with each other. If the <b>no-local-switching</b> statement is configured, frames arriving on a CE interface are sent to a VPLS edge (VE) device or core-facing interfaces only. |
| <div>  <p><b>NOTE:</b> (MX80, MX104, and the 16x10GE MPC, MPC1, or MPC2 on MX240, MX480, MX960, MX2010, and MX2020 only) If you configure the <b>no-local-switching</b> command at the [edit bridge-domains <i>bridge-domain-name</i>] hierarchy level, it might not prevent multicast traffic from being forwarded between the CE-facing interfaces of the bridge domain. Broadcast, unknown unicast, and known multicast traffic does not exhibit this behavior.</p> </div> |                                                                                                                                                                                                                                 |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                             |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>• <a href="#">Configuring VPLS and Integrated Routing and Bridging on page 892</a></li> </ul>                                                                                            |

## no-mac-learning

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | no-mac-learning;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>     | <p>[edit bridge-domains <i>bridge-domain-name</i> bridge-options],</p> <p>[edit bridge-domains <i>bridge-domain-name</i> bridge-options interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> bridge-domains <i>bridge-domain-name</i> bridge-options],</p> <p>[edit logical-systems <i>logical-system-name</i> bridge-domains <i>bridge-domain-name</i> bridge-options interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> bridge-options],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> bridge-options interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> switch-options],</p> <p>[edit logical-systems <i>logical-system-name</i> switch-options],</p> <p>[edit bridge-domains <i>bridge-domain-name</i> bridge-options interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> bridge-options],</p> <p>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> bridge-options interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols evpn],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols evpn <i>interface interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> switch-options],</p> <p>[edit switch-options],</p> <p>[edit switch-options interface <i>interface-name</i>],</p> <p>[set vlans <i>vlan-name</i> switch-options]</p> |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 8.4.</p> <p>Support for the <b>switch-options</b> statement added in Junos OS Release 9.2.</p> <p>Support for top-level configuration for the <b>virtual-switch</b> type of routing instance added in Junos OS Release 9.2. In Junos OS Release 9.1 and earlier, the routing instances hierarchy supported this statement only for a VPLS instance or bridge domain configured within a virtual switch.</p> <p>Support for logical systems added in Junos OS Release 9.6.</p> <p>[edit switch-options], [edit switch-options interface <i>interface-name</i>], [edit vlans <i>vlan-name</i> switch-options], and [edit vlans <i>vlan-name</i> switch-options interface <i>interface-name</i>] hierarchy levels introduced in Junos OS Release 12.3 R2 for EX Series switches.</p> <p>Support for EVPNs added in Junos OS Release 13.2 for MX 3D Series routers.</p> <p>Hierarchy levels [edit switch-options interface <i>interface-name</i>] and [edit vlans <i>vlan-name</i> switch-options] introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>         | <p>For MX Series routers and EX Series switches, disable MAC learning for a virtual switch, for a bridge domain or VLAN, for a specific logical interface in a bridge domain or VLAN, or for a set of bridge domains or VLANs associated with a Layer 2 trunk port. On platforms that support EVPNs, you can disable MAC learning on an EVPN.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



**NOTE:** When MAC learning is disabled for a VPLS routing instance, traffic is not load-balanced and only one of the equal-cost next hops is used.

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>                  | MAC learning is enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring EVPN Routing Instances on page 239</a></li> <li>• <i>Configuring EVPN Routing Instances on EX9200 Switches</i></li> <li>• <i>Understanding Layer 2 Learning and Forwarding for Bridge Domains</i></li> <li>• <i>Layer 2 Learning and Forwarding for VLANs Overview</i></li> <li>• <i>Understanding Layer 2 Learning and Forwarding for Bridge Domains Functioning as Switches with Layer 2 Trunk Ports</i></li> <li>• <i>Understanding Bridging and VLANs on EX Series Switches</i></li> <li>• <i>Understanding Q-in-Q Tunneling on EX Series Switches</i></li> </ul> |

## no-revert (Local Switching)

---

|                     |                                                                                                                                                                                                     |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax              | no-revert;                                                                                                                                                                                          |
| Hierarchy Level     | [edit protocols l2circuit local-switching interfaces <i>interface-name</i> ]<br>[edit protocols l2circuit local-switching interfaces <i>interface-name</i> end-interface<br><i>interface-name</i> ] |
| Release Information | Statement introduced in Junos OS Release 11.4.                                                                                                                                                      |
| Description         | (Optional) Prevent the local switching interface from reverting to the primary interface.                                                                                                           |



**NOTE:** The protect interface must be configured prior to configuring the **no-revert** statement.

Typically, when the primary interface goes down, the pseudowire starts using the protect interface. By default, when the primary interface comes back online, the interface is switched-over back from the protect interface to the primary interface. To prevent the switchover back to the primary interface, unless the primary interface goes down, include the **no-revert** statement. This prevents loss of traffic during the switchover.



**NOTE:** If the protect interface fails, the interface is switched-over back to the primary interface, irrespective of whether or not the **no-revert** statement is included in the configuration.

This statement can be configured both for the starting interface and the ending interface.

|                          |                                                                                                                     |
|--------------------------|---------------------------------------------------------------------------------------------------------------------|
| Required Privilege Level | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration. |
|--------------------------|---------------------------------------------------------------------------------------------------------------------|

|                       |                                                                                                                                         |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Related Documentation | <ul style="list-style-type: none"><li>• <a href="#">Configuring Local Interface Switching in Layer 2 Circuits on page 348</a></li></ul> |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------|

## no-revert (Neighbor Interface)

|                            |                                                                                                                                                                                                                             |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | no-revert;                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>     | [edit protocols l2circuit neighbor <i>address</i> interfaces <i>interface-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interfaces<br><i>interface-name</i> ] |
| <b>Release Information</b> | Statement introduced in Junos OS Release 11.3.                                                                                                                                                                              |
| <b>Description</b>         | (Optional) Prevent the protect interface from reverting to the primary interface.                                                                                                                                           |



**NOTE:** The protect interface must be configured prior to configuring the **no-revert** statement.

Typically, when the primary interface goes down, the pseudowire starts using the protect interface. By default, when the primary interface comes back online, the interface is switched-over back from the protect interface to the primary interface. To prevent the switchover back to the primary interface, unless the protect interface goes down, include the **no-revert** statement. This prevents loss of traffic during the switchover.



**NOTE:** If the protect interface fails, the interface is switched-over back to the primary interface, irrespective of whether or not the **no-revert** statement is included in the configuration.

|                                 |                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Interfaces for Layer 2 Circuits on page 350</a></li> </ul> |

## no-tunnel-services

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | no-tunnel-services;                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>     | [edit logical-systems <i>logical-system-name</i> protocols vpls static-vpls],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls],<br>[edit protocols vpls static-vpls],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls]                                                                                                                                                                             |
| <b>Release Information</b> | Statement introduced in Junos OS Release 7.6.<br>Support for static VPLS added in Junos OS Release 10.2.                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>         | Configure VPLS on a router without a Tunnel Services PIC. Configuring the <b>no-tunnel-services</b> statement creates a label-switched interface (LSI) to provide VPLS functionality. An LSI MPLS label is used as the inner label for VPLS. This label maps to a VPLS routing instance. On the PE router, the LSI label is stripped and then mapped to a logical LSI interface. The Layer 2 Ethernet frame is then forwarded using the LSI interface to the correct VPLS routing instance. |



**NOTE:** In VPLS documentation, the word *Router* in terms such as *PR Router* is used to refer to any device that provides routing functions.

Label-switched interfaces configured with the **no-tunnel-services** statement are not supported with GRE tunnels.



**NOTE:** Although visible in the CLI, the **no-tunnel-services** statement is not supported on DPC cards at the [edit logical-systems *logical-system-name* protocols vpls static-vpls] and the [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vpls] hierarchy levels.

|                                 |                                                                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring VPLS Without a Tunnel Services PIC on page 611</a></li> <li>• <a href="#">Configuring Static Pseudowires for VPLS on page 613</a></li> <li>• <a href="#">Configuring EXP-Based Traffic Classification for VPLS on page 921</a></li> </ul> |



## oam

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> oam {   ping-interval;   bfd-liveness-detection {     detection-time {       threshold <i>milliseconds</i>;     }     minimum-interval <i>milliseconds</i>;     minimum-receive-interval <i>milliseconds</i>;     multiplier <i>number</i>;     no-adaptation;     transmit-interval {       minimum-interval <i>milliseconds</i>;       threshold <i>milliseconds</i>;     }     version <i>bfd-protocol-version</i>;   }   control-channel {     pwe3-control-word;     pseudowire-label-ttl-1;     router-alert-label;   } } </pre> |
| <b>Hierarchy Level</b>          | [edit routing-instances <i>routing-instance-name</i> protocols l2vpn],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i> ],<br>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> ]                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.0.<br>Support for VPLS FEC 129 introduced in Junos OS Release 12.2.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Allows you to configure bidirectional forwarding detection (BFD) and a control channel for a pseudowire, in addition to the corresponding operations and management functions to be used over that control channel. BFD provides a low resource fault detection mechanism for the continuous monitoring of the pseudowire data path and for detecting data plane failures. The <b>control-channel</b> statement is not applicable to Layer 2 circuit pseudowires.                                                                            |
| <b>Options</b>                  | The <b>bfd-liveness-detection</b> statement and substatements are described in the <i>Junos OS Routing Protocols Library</i> .<br><br>The other statements are explained separately.                                                                                                                                                                                                                                                                                                                                                         |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring BFD for VCCV for Layer 2 VPNs, Layer 2 Circuits, and VPLS on page 188</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                        |

## packet-action

**Syntax** `packet-action action;`

**Hierarchy Level** [edit bridge-domains *bridge-domain-name* bridge-options interface *interface-name* interface-mac-limit *limit*],  
 [edit bridge-domains *bridge-domain-name* bridge-options interface-mac-limit *limit*],  
 [edit logical-systems *logical-system-name* bridge-domains *bridge-domain-name* bridge-options interface *interface-name* interface-mac-limit *limit*],  
 [edit logical-systems *logical-system-name* bridge-domains *bridge-domain-name* bridge-options interface-mac-limit *limit*],  
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* bridge-domains *bridge-domain-name* bridge-options interface *interface-name* interface-mac-limit *limit*],  
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* bridge-domains *bridge-domain-name* bridge-options interface-mac-limit *limit*],  
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* switch-options interface *interface-name* interface-mac-limit *limit*],  
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* switch-options interface-mac-limit *limit*],  
 [edit logical-systems *logical-system-name* switch-options interface-mac-limit *limit*],  
 [edit protocols l2-learning global-mac-limit *limit*],  
 [edit routing-instances *routing-instance-name* bridge-domains *bridge-domain-name* bridge-options interface *interface-name* interface-mac-limit *limit*],  
 [edit routing-instances *routing-instance-name* bridge-domains *bridge-domain-name* bridge-options interface-mac-limit *limit*],  
 [edit routing-instances *routing-instance-name* protocols evpn [interface-mac-limit \(VPLS\)](#)],  
 [edit routing-instances *routing-instance-name* protocols evpn interface *interface-name* [interface-mac-limit \(VPLS\)](#)],  
 [edit routing-instances *routing-instance-name* protocols evpn [mac-table-size limit](#)],  
 [edit routing-instances *routing-instance-name* switch-options interface *interface-name* interface-mac-limit *limit*],  
 [edit routing-instances *routing-instance-name* switch-options interface-mac-limit *limit*],  
 [edit switch-options interface-mac-limit *limit*],  
 [edit switch-options interface *interface-name* interface-mac-limit *limit*],  
 [edit switch-options interface-mac-limit *limit*],  
 [edit switch-options interface *interface-name* interface-mac-limit *limit*],  
 [edit switch-options interface-mac-limit *limit*],  
 [edit switch-options mac-table-size *limit*],  
 [edit switch-options interface *interface-name* interface-mac-limit *limit*],  
 [edit vlans *vlan-name* switch-options interface *interface-name* interface-mac-limit *limit*],  
 [edit vlans *vlan-name* switch-options interface-mac-limit *limit*],  
 [edit vlans *vlan-name* switch-options mac-table-size *limit*]  
 [edit vlans *vlan-name* switch-options interface-mac-limit *limit*],  
 [edit vlans *vlan-name* switch-options interface *interface-name* interface-mac-limit *limit*],  
 [edit vlans *vlan-name* switch-options mac-table-size *limit*]

**Release Information** Statement introduced in Junos OS Release 8.4.  
 Support for the **switch-options** statement added in Junos OS Release 9.2.  
 Support for top-level configuration for the **virtual-switch** type of routing instance added in Junos OS Release 9.2. In Junos OS Release 9.1 and earlier, the routing instances hierarchy supported this statement only for a VPLS instance or a bridge domain configured within a virtual switch.

Support for logical systems added in Junos OS Release 9.6.

[edit switch-options interface *interface-name* interface-mac-limit *limit*], [edit switch-options interface-mac-limit *limit*], [edit switch-options mac-table-size *limit*], [edit vlans *vlan-name* switch-options interface *interface-name* interface-mac-limit *limit*], [edit vlans *vlan-name* switch-options interface-mac-limit *limit*], and [edit vlans *vlan-name* switch-options mac-table-size *limit*] hierarchy levels introduced in Junos OS Release 12.3R2 for EX Series switches.

Support for EVPNs introduced in Junos OS Release 13.2 on MX Series 3D Universal Edge Routers.

Support at the [edit switch-options interface *interface-name* interface-mac-limit *limit*] hierarchy level and hierarchy levels under [edit vlans *vlan-name*] introduced in Junos OS Release 13.2X50-D10 for EX Series switches and Junos OS Release 13.2 for the QFX Series.

**Description** Specify the action taken when packets with new source MAC addresses are received after the MAC address limit is reached. If this statement is not configured, packets with new source MAC addresses are forwarded by default.

**Default**



**NOTE:** On a QFX Series Virtual Chassis, if you include the shutdown option at the [edit vlans *vlan-name* switch-options interface *interface-name* interface-mac-limit packet-action] hierarchy level and issue the commit operation, the system generates a commit error. The system does not generate an error if you include the shutdown option at the [edit switch-options interface *interface-name* interface-mac-limit packet-action] hierarchy level.

Disabled. The default is for packets for new source MAC addresses to be forwarded after the MAC address limit is reached.

**Options**

- drop**—Drop packets with new source MAC addresses, and do not learn the new source MAC addresses.
- drop-and-log**—(EX Series switches and QFX Series only) Drop packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry.
- log**—(EX Series switches and QFX Series only) Hold packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry.
- none**—(EX Series switches and QFX Series only) Forward packets with new source MAC addresses, and learn the new source MAC address.
- shutdown**—(EX Series switches and QFX Series only) Disable the specified interface, and generate an alarm, an SNMP trap, or a system log entry.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related  
Documentation**

- [Configuring EVPN Routing Instances on page 239](#)
- *Configuring EVPN Routing Instances on EX9200 Switches*
- *Configuring MAC Limiting (CLI Procedure)*
- *Configuring Persistent MAC Learning (CLI Procedure)*
- *Understanding Layer 2 Learning and Forwarding for Bridge Domains*
- *Layer 2 Learning and Forwarding for VLANs Overview*
- *Understanding Layer 2 Learning and Forwarding for Bridge Domains Functioning as Switches with Layer 2 Trunk Ports*
- *Layer 2 Learning and Forwarding for VLANs Overview*
- *Layer 2 Learning and Forwarding for VLANs Acting as a Switch for a Layer 2 Trunk Port*

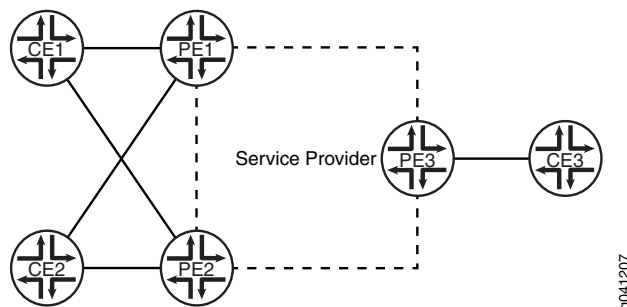
## peer-active (VPLS Multihoming for FEC 129)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>peer-active;</code>                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>     | <pre>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls multi-homing], [edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls multi-homing site <i>site-name</i>], [edit routing-instances <i>instance-name</i> protocols vpls multi-homing], [edit routing-instances <i>instance-name</i> protocols vpls multi-homing site <i>site-name</i>]</pre> |
| <b>Release Information</b> | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>         | Keep customer edge (CE) interfaces in the up state when all BGP peers go down.                                                                                                                                                                                                                                                                                                                                                                          |



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

Consider a scenario in which two provider edge (PE) routers are sharing two multihomed sites under one routing instance, with two CE devices, CE1 and CE2.



If the BGP peering session drops between Router PE1 and Router PE2, each one would consider itself to be the designated forwarder (DF) for Device CE1 and Device CE2. This creates a loop through the two CE devices, in which traffic loops from one CE device to the other then back to the first.

Junos OS overcomes this scenario by dropping all multihomed CE interface traffic on all multihoming PE routers when the BGP session drops between the PE routers. This functionality is enabled by default for all sites in a routing instance.

The **peer-active** statement disables the default functionality, so that PE routers keep their multihomed CE interfaces in the up state, even though the BGP peering session is down.


If you configure this statement in the **multi-homing** hierarchy, the default functionality is disabled for all sites. If you configure this statement for a site, the default functionality is disabled only for that particular site.

|                                 |                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>                  | If you omit this statement, Junos OS drops all multihomed CE interface traffic on all multihoming PE routers when the BGP session drops between the PE routers. |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Example: Configuring VPLS Multihoming (FEC 129) on page 767</a></li></ul>                                   |

---

## peer-as (VPLS)

---

|                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                   | peer-as {<br>all;<br>}                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> ] |
| <b>Release Information</b>                                                                                                                                                                                                                                      | Statement introduced in Junos OS Release 9.3.                                                                                                                                                                                                                  |
| <b>Description</b>                                                                                                                                                                                                                                              | Enable the autonomous system border router (ASBR) to establish a single pseudowire to each of the other ASBRs interconnected using inter-AS VPLS with MAC processing at the ASBR.                                                                              |
| <div> <b>NOTE:</b> In the VPLS documentation, the word <i>router</i> in terms such as <i>PE router</i> is used to refer to any device that provides routing functions.</div> |                                                                                                                                                                                                                                                                |
| <b>Options</b>                                                                                                                                                                                                                                                  | all—This option is required. All peer routers, the ASBRs, are placed within the same VPLS mesh group.                                                                                                                                                          |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                 | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                            |
| <b>Related Documentation</b>                                                                                                                                                                                                                                    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Inter-AS VPLS with MAC Processing at the ASBR on page 559</a></li></ul>                                                                                                                        |

## ping-interval

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>ping-interval seconds;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | <p>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> oam],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols l2vpn oam],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls neighbor <i>address</i> oam],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>address</i> oam],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls oam],</p> <p>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> oam],</p> <p>[edit routing-instances <i>instance-name</i> protocols l2vpn oam],</p> <p>[edit routing-instances <i>instance-name</i> protocols vpls neighbor <i>address</i> oam],</p> <p>[edit routing-instances <i>instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>address</i> oam],</p> <p>[edit routing-instances <i>instance-name</i> protocols vpls oam]</p> |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 10.0.</p> <p>Support for FEC 129 VPLS added in Junos OS Release 12.2.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | Configure the time interval between ping messages for bidirectional forwarding detection (BFD) sessions enabled over pseudowires inside a VPN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <p><i>seconds</i>—Time interval between ping messages.</p> <p><b>Range:</b> 30 through 3600</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">Configuring BFD for VCCV for Layer 2 VPNs, Layer 2 Circuits, and VPLS on page 188</a> in the <i>Junos OS VPNs Library for Routing Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## policer (Layer 2 VPN)

---

|                                 |                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>policer {<br/>    input <i>policer-template-name</i>;<br/>    output <i>policer-template-name</i>;<br/>}</pre>                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family (ccc   inet   tcc)],<br>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family (ccc   inet   tcc)]                                                              |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                               |
| <b>Description</b>              | Use policing to control the amount of traffic flowing over the interfaces servicing a Layer 2 VPN.                                                                                                                                                                                                              |
| <b>Options</b>                  | <p><b>input <i>policer-template-name</i></b>—Name of one policer to evaluate when packets are received on the interface.</p> <p><b>output <i>policer-template-name</i></b>—Name of one policer to evaluate when packets are transmitted on the interface.</p>                                                   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Traffic Policing in Layer 2 VPNs on page 183</a></li><li>• <i>Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices</i></li><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li></ul> |



## preference (Interface-Level Preference for VPLS Multihoming for FEC 129)


|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>preference <i>preference-value</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls multi-homing site <i>site-name</i> interface <i>interface-name</i> ],<br>[edit routing-instances <i>instance-name</i> protocols vpls multi-homing site <i>site-name</i> interface <i>interface-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>              | <p>Specify a preference for the interface to become the designated forwarder (DF) for a multihomed VPLS site. This <b>preference</b> statement can be useful when you want the interface preference for a site to change dynamically so that the DF election can be influenced depending on the interface state. Among the list of interface preferences, Junos OS advertises the best preference as the VPLS site's preference value. For example, if the site has three interfaces configured with preference values 12, 10, and 9, respectively, 12 is advertised as the site preference. If that interface goes down, 10 is advertised as the site preference.</p> <p>If you configure interface-level preference, you cannot configure site-level preference.</p> |
| <b>Options</b>                  | <p><b><i>preference-value</i></b>—Preference value for the interface.</p> <p><b>Range:</b> 1 through 65535</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring VPLS Multihoming (FEC 129) on page 767</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## preference (Site-Level Preference for VPLS Multihoming for FEC 129)

---

|                                 |                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>preference (<i>preference-value</i>   backup   primary);</code>                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls multi-homing site <i>site-name</i> ],<br>[edit routing-instances <i>instance-name</i> protocols vpls multi-homing site <i>site-name</i> ] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                   |
| <b>Description</b>              | Influence the designated forwarder (DF) selection for a multihomed VPLS site. Configure the preference in terms of keywords <b>primary</b> and <b>backup</b> , or configure the preference value explicitly.                                     |
| <b>Default</b>                  | If this statement is omitted, the default preference value for the site is 100.                                                                                                                                                                  |
| <b>Options</b>                  | <b><i>preference-value</i></b> —Preference value for the DF.<br><b>Range:</b> 1 through 65535<br><b>backup</b> —Less likely to become the DF.<br><b>primary</b> —Most likely to become the DF.                                                   |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Example: Configuring VPLS Multihoming (FEC 129) on page 767</a></li></ul>                                                                                                                    |

## primary (VPLS Multihoming)

|                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                            | <code>primary interface-name;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                   | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls multi-homing active-interface],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls multi-homing site <i>site-name</i> active-interface],</p> <p>[edit routing-instances <i>instance-name</i> protocols vpls multi-homing active-interface],</p> <p>[edit routing-instances <i>instance-name</i> protocols vpls multi-homing site <i>site-name</i> active-interface]</p> |
| <b>Release Information</b>                                                                                                                                                                                                                                               | Statement introduced in Junos OS Release 7.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>                                                                                                                                                                                                                                                       | <p>Specify the name of the multihomed interface to be used as the primary interface by the VPLS site.</p> <p>For FEC 128, use the [edit routing-instances <i>instance-name</i> protocols vpls multi-homing active-interface] hierarchy level.</p>                                                                                                                                                                                                                                                                                            |
| <b>Default</b>                                                                                                                                                                                                                                                           | If you omit this statement, depending on the order in which interfaces are listed in the PE router's configuration, the first operational interface in the set of configured interfaces is chosen to be the primary interface.                                                                                                                                                                                                                                                                                                               |
| <div>  <p><b>NOTE:</b> In the VPLS documentation, the word <i>router</i> in terms such as <i>PE router</i> is used to refer to any device that provides routing functions.</p> </div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                                                                                                                                                                                                                                                           | <i>interface-name</i> —Name of the interface (for example, <code>ge-0/1/0.1</code> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                          | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>                                                                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>• <a href="#">Specifying an Interface as the Active Interface on page 754</a></li> <li>• <a href="#">any on page 1071</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                  |

## protect-interface

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>protect-interface <i>interface-name</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | <code>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],</code><br><code>[edit logical-systems <i>logical-system-name</i> protocols l2circuit local-switching interface <i>interface-name</i>],</code><br><code>[edit logical-systems <i>logical-system-name</i> protocols l2circuit local-switching interface <i>interface-name</i> end-interface],</code><br><code>[edit protocols l2circuit local-switching interface <i>interface-name</i>],</code><br><code>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],</code><br><code>[edit protocols l2circuit local-switching interface <i>interface-name</i> end-interface]</code> |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Provide a backup for the protected interface in case of failure. Network traffic uses the primary interface only, as long as the primary interface functions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <i>interface-name</i> —Name of the protect interface to configure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Protect Interface on page 353</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## protected-l2circuit

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | protected-l2circuit {<br>egress-pe <i>address</i> ;<br>ingress-pe <i>address</i> ;<br>virtual-circuit-id <i>identifier</i> ;<br>}                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> <b>egress-protection</b> ],<br>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> <b>egress-protection</b> ]                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS release 10.4.                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | Configures the protected Layer 2 circuit as part of an egress protection virtual circuit (EPVC).                                                                                                                                                                                                                                                                           |
| <b>Options</b>                  | <p><b>egress-pe <i>address</i></b>—Specify the address of the egress PE router for the protected Layer 2 circuit.</p> <p><b>ingress-pe <i>address</i></b>—Specify the address of the ingress PE router for the protected Layer 2 circuit.</p> <p><b>virtual-circuit-id <i>identifier</i></b>—Specify the virtual circuit identifier for the protected Layer 2 circuit.</p> |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring an Egress Protection LSP for a Layer 2 Circuit on page 404</a></li> </ul>                                                                                                                                                                                                                        |

## protector-interface

---

|                                 |                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>protector-interface <i>interface-name</i>;</code>                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> <b>egress-protection</b> ],<br>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> <b>egress-protection</b> ] |
| <b>Release Information</b>      | Statement introduced in Junos OS release 10.4.                                                                                                                                                                                                                           |
| <b>Description</b>              | Configures the protector interface for an egress protection LSP.                                                                                                                                                                                                         |
| <b>Options</b>                  | <i>interface-name</i> —Name of the interface used to protect traffic for an egress protection LSP.                                                                                                                                                                       |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Example: Configuring an Egress Protection LSP for a Layer 2 Circuit on page 404</a></li></ul>                                                                                                                        |

## protector-pe

---

|                                 |                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>protector-pe <i>address</i> {<br/>    context-identifier <i>identifier</i>;<br/>    lsp <i>lsp-name</i>;<br/>}</pre>                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> <b>egress-protection</b> ],<br>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> <b>egress-protection</b> ] |
| <b>Release Information</b>      | Statement introduced in Junos OS release 10.4.                                                                                                                                                                                                                           |
| <b>Description</b>              | Configures the protector PE router for an egress protection LSP. Test.                                                                                                                                                                                                   |
| <b>Options</b>                  | <i>address</i> —IPv4 address for the protector PE router.<br><br><i>context-identifier identifier</i> —Identifies the context for the egress protection LSP.<br><br><i>lsp lsp-name</i> —Specifies the LSP for the egress protection LSP.                                |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Example: Configuring an Egress Protection LSP for a Layer 2 Circuit on page 404</a></li></ul>                                                                                                                        |

## proxy (Interfaces)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>proxy inet-address <i>address</i>;</code>                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family tcc],<br>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family tcc]                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | For Layer 2.5 VPNs using an Ethernet interface as the TCC router, configure the IP address for which the TCC router is proxying. Ethernet TCC is supported on interfaces that carry IPv4 traffic only. Ethernet TCC encapsulation is supported on 1-port Gigabit Ethernet, 2-port Gigabit Ethernet, 4-port Gigabit Ethernet, and 4-port Fast Ethernet PICs only. Ethernet TCC is not supported on the T640 routing node. |
| <b>Options</b>                  | <code>inet-address <i>address</i></code> —IP address for which the TCC router is acting as a proxy.                                                                                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring TCC Encapsulation for Layer 2 VPNs and Layer 2 Circuits on page 164</a></li> </ul>                                                                                                                                                                                                                                                                      |

## pseudowire-status-tlv

|                                 |                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>pseudowire-status-tlv <a href="#">hot-standby-vc-on</a>;</code>                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> ],<br>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> ],                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.0.                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | <p>Enables the pseudowire type length variable (TLV). The pseudowire status TLV is used to communicate the status of a pseudowire back and forth between two PE routers. The pseudowire status TLV is configurable for each pseudowire connection and is disabled by default.</p> <p>The remaining statement is explained separately.</p> |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Pseudowire Status TLV on page 354</a></li> <li>• <a href="#">Example: Configuring Pseudowire Redundancy in a Mobile Backhaul Scenario on page 371</a></li> </ul>                                                                                                     |

## psn-tunnel-endpoint

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>psn-tunnel-endpoint address;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | <code>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],</code><br><code>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> backup-neighbor <i>address</i>],</code><br><code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i> backup-neighbor <i>address</i>],</code><br><code>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],</code><br><code>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> backup-neighbor <i>address</i>],</code><br><code>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i> backup-neighbor <i>address</i>]</code> |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Hierarchy levels associated with the <b>backup-neighbor</b> statement added in Junos OS Release 9.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | Specify the endpoint of the packet switched network (PSN) tunnel on the remote PE router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <b>address</b> —Address for the tunnel endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Required Privilege Level</b> | <code>routing</code> —To view this statement in the configuration.<br><code>routing-control</code> —To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Layer 2 Circuits over Both RSVP and LDP LSPs on page 355</a></li><li>• <a href="#">Configuring Pseudowire Redundancy on the PE Router on page 180</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |



## remote

|                                 |                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>remote (inet-address   mac-address) address;</code>                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family tcc],<br>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family tcc]                                                                                                                               |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | For Layer 2.5 VPNs employing an Ethernet interface as the TCC router, configure the location of the remote router. Ethernet TCC is supported on interfaces that carry IPv4 traffic only. Ethernet TCC encapsulation is supported on 1-port Gigabit Ethernet, 2-port Gigabit Ethernet, 4-port Gigabit Ethernet, and 4-port Fast Ethernet PICs only. |
| <b>Options</b>                  | <b>inet-address</b> <i>address</i> —The IP address of the remote site.<br><br><b>mac-address</b> <i>address</i> —The MAC address of the remote site.                                                                                                                                                                                               |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring TCC Encapsulation for Layer 2 VPNs and Layer 2 Circuits on page 164</a></li> </ul>                                                                                                                                                                                                |

## remote-site-id

|                                 |                                                                                                                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>remote-site-id remote-site-ID;</code>                                                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i> interface <i>interface-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i> interface <i>interface-name</i> ] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 11.1 for EX Series switches.                                                                                                                                                                               |
| <b>Description</b>              | Control the remote interface to which the interface should connect. If you do not explicitly configure the remote site ID, the order of the interfaces configured for the site determines the default value. This statement is optional.                                                                 |
| <b>Options</b>                  | <b>remote-site-ID</b> —Identifier specifying the interface on the remote PE router the Layer 2 VPN routing instance connects to.                                                                                                                                                                         |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Remote Site ID on page 128</a></li> <li>• <a href="#">Configuring an MPLS-Based Layer 2 VPN (CLI Procedure)</a></li> </ul>                                                                                                          |

## routing-instances

---

|                                 |                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>routing-instances <i>routing-instance-name</i> { ... }</code>                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit],<br>[edit logical-systems <i>logical-system-name</i> ]                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                        |
| <b>Description</b>              | Configure an additional routing entity for a router or switch. You can create multiple instances of BGP, IS-IS, OSPF, OSPF version 3 (OSPFv3), and RIP for a router or switch.                           |
| <b>Default</b>                  | Routing instances are disabled for the router or switch.                                                                                                                                                 |
| <b>Options</b>                  | <i>routing-instance-name</i> —Name of the routing instance, a maximum of 31 characters. The remaining statements are explained separately.                                                               |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring EVPN Routing Instances on page 239</a></li><li>• <a href="#">Configuring Routing Instances on PE Routers in VPNs on page 9</a></li></ul> |

## rsvp-te (Routing Instances Provider Tunnel)

|                                 |                                                                                                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>rsvp-te {   label-switched-path-template {     (default-template   <i>lsp-template-name</i>);   }   static-lsp <i>lsp-name</i>; }</pre>                                                                       |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel],<br>[edit routing-instances <i>routing-instance-name</i> provider-tunnel]                         |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.3.                                                                                                                                                                      |
| <b>Description</b>              | Configure VPLS unknown unicast, broadcast, and multicast traffic flooding using point-to-multipoint LSPs.                                                                                                          |
| <b>Options</b>                  | <p><b>static-lsp <i>lsp-name</i></b>—Create a static point-to-multipoint LSP and automatically include all of the neighbors in the VPLS routing instance.</p> <p>The remaining option is explained separately.</p> |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Flooding Unknown Traffic Using Point-to-Multipoint LSPs in VPLS on page 847</a></li> </ul>                                                                    |

## send-oam

|                                 |                                                                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | send-oam;                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit protocols l2circuit neighbor address interface interface-name <b>static</b> ]                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.5.<br>Statement introduced in Junos OS Release 12.1x48 for PTX Series Packet Transport Routers.<br>Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Access Routers.                                  |
| <b>Description</b>              | Enable the ability to ping a static pseudowire. If you configure the <b>send-oam</b> statement, it applies to the backup neighbor as well. Once you have configured this statement, you can ping the static pseudowire by issuing the <b>ping mpls l2circuit</b> command. |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Static Layer 2 Circuits on page 347</a></li> <li>• <a href="#">ping mpls l2circuit on page 1244</a></li> </ul>                                                                                           |

## site (Layer 2 Circuits)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>site <i>site-name</i> {<br/>    hot-standby;<br/>    site-identifier <i>identifier</i>;<br/>    site-preference <i>preference-value</i> {<br/>        backup;<br/>        primary;<br/>    }<br/>    interface <i>interface-name</i> {<br/>        description <i>text</i>;<br/>        remote-site-id <i>remote-site-ID</i>;<br/>    }<br/>}</pre>                                                          |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn],<br>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn]                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 11.1 for EX Series switches.<br><b>hot-standby</b> option introduced in Junos OS Release 14.2 for MX Series routers.                                                                                                                                                                                                |
| <b>Description</b>              | Specify the site name, site identifier, and interfaces connecting to the site. Allows you to configure a remote site ID for remote sites.                                                                                                                                                                                                                                                                         |
| <b>Options</b>                  | <p><b>hot-standby</b>—Turn on the protector behavior for the site. This keeps backup pseudowire in continuous standby mode and ready for traffic forwarding.</p> <p><b>site-identifier <i>identifier</i></b>—Numerical identifier for the site used as a default reference for the remote site ID.</p> <p><b><i>site-name</i></b>—Name of the site.</p> <p>The remaining statements are explained separately.</p> |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Site on page 127</a></li><li>• <a href="#">Configuring an MPLS-Based Layer 2 VPN (CLI Procedure)</a></li></ul>                                                                                                                                                                                                                                |

## site (VPLS Multihoming for FEC 128)

|                                 |                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> site <i>site-name</i> {   active-interface (<i>any</i>   <i>primary interface-name</i>);   best-site;   interface <i>interface-name</i> {     interface-mac-limit <i>limit</i>;   }   mesh-group <i>mesh-group-name</i>;   multi-homing;   site-identifier <i>identifier</i>;   site-preference <i>preference-value</i>; } </pre> |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols <i>vpls</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols <i>vpls</i> ]                                                                                                                                |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | Specify the site name and site identifier for a site. Allows you to configure a remote site ID for remote sites.                                                                                                                                                                                                                        |
| <b>Options</b>                  | <p><i>site-name</i>—Name of the site.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                     |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the VPLS Site Name and Site Identifier on page 565</a></li> </ul>                                                                                                                                                                                                      |

## site (VPLS Multihoming for FEC 129)

---

**Syntax**    `site site-name {  
          active-interface interface-name {  
            any;  
            primary interface-name;  
          }  
          identifier identifier;  
          interface interface-name {  
            preference preference-value;  
          }  
          peer-active;  
          preference (preference-value | backup | primary);  
          }`

**Hierarchy Level**    [edit logical-systems *logical-system-name* routing-instances *instance-name* protocols vpls **multi-homing**],  
                          [edit routing-instances *instance-name* protocols vpls **multi-homing**]

**Release Information**    Statement introduced in Junos OS Release 12.3.

**Description**    For VPLS autodiscovery (FEC 129), specify the parameters for a VPLS site that is multihomed to two or more provider edge (PE) routers.



**NOTE:** In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

---

**Options**    ***site-name***—Name of the site.

The remaining statements are explained separately.

**Required Privilege**    routing—To view this statement in the configuration.  
**Level**    routing-control—To add this statement to the configuration.

**Related Documentation**

- [Example: Configuring VPLS Multihoming \(FEC 129\) on page 767](#)

## site-identifier (Layer 2 Circuits)

|                                 |                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>site-identifier <i>identifier</i>;</code>                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i> ] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 11.1 for EX Series switches.                                                                                                               |
| <b>Description</b>              | Specify the numerical identifier for the local Layer 2 VPN site.                                                                                                                                                                         |
| <b>Options</b>                  | <i>identifier</i> —The numerical identifier for the Layer 2 VPN site, which can be any number from 1 through 65,534.                                                                                                                     |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Site on page 127</a></li> <li>• <a href="#">Configuring an MPLS-Based Layer 2 VPN (CLI Procedure)</a></li> </ul>                                                    |

## site-identifier (VPLS)

|                                 |                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>site-identifier <i>identifier</i>;</code>                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i> ] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                      |
| <b>Description</b>              | Specify the numerical identifier for the local VPLS site.                                                                                                                                                                              |
| <b>Options</b>                  | <i>identifier</i> —Specify the numerical identifier for the local VPLS site. The identifier must be an unsigned 16-bit number greater than zero.                                                                                       |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the VPLS Site Name and Site Identifier on page 565</a></li> </ul>                                                                                                     |

## site-preference

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>site-preference <i>preference-value</i> {<br/>    backup;<br/>    primary;<br/>}</code>                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i> ] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced for Layer 2 VPNs in Junos OS Release 9.1.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | Specify the preference value advertised for a particular Layer 2 VPN or VPLS site. The site preference value is encoded in the BGP local preference attribute. When a PE router receives multiple advertisements with the same VE identifier, the advertisement with the highest local preference value is preferred. You can use this statement to enable multihoming for Layer 2 VPNs and VPLS.                                                                                   |
| <b>Options</b>                  | <b><i>preference-value</i></b> —Specify the preference value advertised for a Layer 2 VPN or VPLS site.<br><b>Range:</b> 1 through 65,535<br><br><b>backup</b> —Set the preference value to 1.<br><br><b>primary</b> —Set the preference value to 65,535.                                                                                                                                                                                                                           |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring a Site Preference and Layer 2 VPN Multihoming on page 130</a></li><li>• <a href="#">Configuring the VPLS Site Preference on page 569</a></li></ul>                                                                                                                                                                                                                                                                  |



## site-range

---

|                                 |                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>site-range <i>number</i>;</code>                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls]                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | Specify an upper limit on the maximum site identifier that can be accepted to allow a pseudowire to be brought up. Pseudowires cannot be established to sites with site identifiers greater than the configured site range. If you issue the <b>show vpls connections</b> command, such sites are displayed as OR (out of range). |
| <b>Options</b>                  | <b><i>number</i></b> —Maximum number of site identifiers. We recommend using the default value.<br><b>Range:</b> 1 through 65,534<br><b>Default:</b> 65,534                                                                                                                                                                       |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Site Range on page 566</a></li> </ul>                                                                                                                                                                                                                        |

## source-attachment-identifier (Protocols VPWS)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>source-attachment-identifier <i>identifier</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn site <i>site-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | <p>For FEC 129, specify the VPWS source attachment identifier. The point-to-point nature of VPWS requires that you specify the source access individual identifier (SAII) and the target access individual identifier (TAII). This SAII-TAII pair defines a unique pseudowire between two PE devices.</p> <p>Auto-discovery routes are used by BGP to allow auto-discovery of remote source access individual identifiers (SAIIs) (the sources of the point-to-point pseudowires). One auto-discovery route is advertised for each source attachment identifier (SAI) in the instance or mesh group.</p> <p>The SAII is specified with the <b>source-attachment-identifier</b> statement within the FEC 129 VPWS routing instance. You configure the source attachment identifier and the interfaces to associate with that source attachment identifier. Under each interface, you can configure the TAII with the <b>target-attachment-identifier</b> statement. If the configured target identifier matches a source identifier advertised by a remote PE device by way of a BGP auto-discovery message, the pseudowire between that source-target pair is signaled. If there is no match between an advertised source identifier and the configured target identifier, the pseudowire is not established.</p> |
| <b>Options</b>                  | <p><b><i>identifier</i></b>—The numerical identifier for the Layer 2 VPN site.</p> <p><b>Range:</b> 1 through 4,292,967,295</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Example: Configuring FEC 129 BGP Autodiscovery for VPWS on page 708</a></li><li>• <a href="#">target-attachment-identifier on page 1203</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## standby (Protocols Layer 2 Circuit)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | standby;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | <p>[edit logical-systems <i>logical-system-name</i> protocols l2circuit local-switching interface <i>interface-name</i> end-interface interface <i>interface-name</i> backup-neighbor <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> backup-neighbor <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i> backup-neighbor <i>address</i>],</p> <p>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> backup-neighbor <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i> backup-neighbor <i>address</i>]</p> |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Hierarchy levels associated with the <b>backup-neighbor</b> statement added in Junos OS Release 9.2.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | <p>Configure the pseudowire to the specified backup neighbor as the standby. When you configure this statement, traffic flows over both the active and standby pseudowires to the backup device (either a CE device or PE router). The backup device drops the traffic from the standby pseudowire, unless the active pseudowire fails. If the active pseudowire fails, the backup device automatically switches to the standby pseudowire.</p> <p>The <b>standby</b> statement is quite similar to the <b>hot-standby</b> statement introduced in Junos OS Release 12.3. The <b>hot-standby</b> statement allows for a faster forwarding-path switchover during transition periods, as compared to what is allowed by the <b>standby</b> statement.</p>                                                                    |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Layer 2 Circuits over Both RSVP and LDP LSPs on page 355</a></li> <li>• <a href="#">Configuring Pseudowire Redundancy on the PE Router on page 180</a></li> <li>• <a href="#">Example: Configuring Layer 2 Circuit Switching Protection on page 420</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## static (Protocols Layer 2 Circuit)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>static {<br/>    incoming-label <i>label</i>;<br/>    outgoing-label <i>label</i>;<br/>    send-oam;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | <pre>[edit logical-systems <i>logical-system-name</i> l2circuit neighbor <i>address</i> interface<br/>  <i>interface-name</i>],<br/>[edit logical-systems <i>logical-system-name</i> l2circuit neighbor <i>address</i> interface <i>interface-name</i><br/>  backup-neighbor <i>neighbor</i>],<br/>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],<br/>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> backup-neighbor <i>neighbor</i>]</pre> |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.5.</p> <p>Statement introduced in Junos OS Release 12.1X48 for PTX Series routers.</p> <p>Statement introduced in Junos OS Release 12.2 for ACX Series routers.</p>                                                                                                                                                                                                                                                                                                   |
| <b>Description</b>              | <p>Configures static Layer 2 circuit pseudowires. Static pseudowires are designed for networks that do not support LDP or do not have LDP enabled. You configure a static pseudowire by configuring static values for the in and out labels needed to enable a pseudowire connection.</p>                                                                                                                                                                                                                           |
| <b>Options</b>                  | <p><b>incoming-label</b>—(Optional for PTX Series Packet Transport Routers only) Configure the Layer 2 circuit incoming static pseudowire label.</p> <p><b>Range:</b> 1000000 through 1048575</p> <p><b>outgoing-label</b>—(Optional for PTX Series Packet Transport Routers only) Configure the Layer 2 circuit outgoing static pseudowire label.</p> <p><b>Range:</b> 16 through 1048575</p> <p>The remaining statement is explained separately.</p>                                                              |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Static Layer 2 Circuits on page 347</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                   |

## static (Protocols VPLS)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | static {<br>incoming-label <i>label</i> ;<br>outgoing-label <i>label</i> ;<br>}                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>address</i> ],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i> ],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i> backup-neighbor <i>address</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>address</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>address</i> backup-neighbor <i>address</i> ] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | Specifies a static pseudowire for a VPLS domain. By configuring static pseudowires for the VPLS domain, you do not need to configure the LDP or BGP protocols that would normally be used for signaling. Static pseudowires require that you configure a set of in and out labels for each pseudowire configured for the VPLS domain. You can configure both static and dynamic neighbors within the same VPLS routing instance. You can also configure a static pseudowire for a backup neighbor (if you configure the neighbor as static the backup must also be static) and for a mesh group.                                                                                                                                                                                                                                                                           |
| <b>Options</b>                  | <b>incoming-label <i>label</i></b> —You must configure an incoming label for the static pseudowire.<br><b>Range:</b> 29,696 through 41,983 and 1,000,000 through 1,048,575<br><br><b>outgoing-label <i>label</i></b> —You must configure an outgoing label for the static pseudowire.<br><b>Range:</b> 16 through 1,048,575                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>See <a href="#">Configuring Static Pseudowires for VPLS on page 613</a>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## static-mac

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>static-mac <i>mac-address</i> {<br/>    vlan-id <i>number</i>;<br/>}</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit bridge-domains <i>bridge-domain-name</i> bridge-options interface <i>interface-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> bridge-domains <i>bridge-domain-name</i><br>bridge-options interface <i>interface-name</i> ],<br>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i><br>bridge-domains <i>bridge-domain-name</i> bridge-options interface <i>interface-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i><br>bridge-options interface <i>interface-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> protocols evpn interface <i>interface-name</i> ]<br>[edit vlans <i>vlan-name</i> switch-options interface <i>interface-name</i> ] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.4.<br>Support for logical systems added in Junos OS Release 9.6.<br>[edit vlans <i>vlan-name</i> switch-options interface <i>interface name</i> ] hierarchy level introduced in Junos OS Release 12.3R2 for EX Series switches.<br>Support for EVPNs added in Junos OS Release 13.2 for MX 3D Series routers. The <b>vlan-id</b> option is not available for EVPNs.<br>[edit vlans <i>vlan-name</i> switch-options interface <i>interface name</i> ] hierarchy level introduced in Junos OS Release 13.2 for the QFX Series.                                                                                                                                                                                                                             |
| <b>Description</b>              | Configure a static MAC address for a logical interface in a bridge domain or VLAN.<br><br>The <b>vlan-id</b> option can be specified for <b>static-macs</b> only if <b>vlan-id all</b> is configured for the bridging domain or VLAN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                  | <b><i>mac-address</i></b> —MAC address<br><br><b><i>vlan-id number</i></b> —(Optional) VLAN identifier to associate with static MAC address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring EVPN Routing Instances on page 239</a></li><li>• <a href="#">Understanding Layer 2 Learning and Forwarding for Bridge Domains</a></li><li>• <a href="#">Layer 2 Learning and Forwarding for VLANs Overview</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## target-attachment-identifier (Protocols VPWS)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>target-attachment-identifier <i>identifier</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols l2vpn site <i>site-name</i> interface <i>interface-name</i> ],<br>[edit routing-instances <i>instance-name</i> protocols l2vpn site <i>site-name</i> interface <i>interface-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>              | <p>For FEC 129, specify the VPWS target attachment identifier. The point-to-point nature of VPWS requires that you specify the source access individual identifier (SAII) and the target access individual identifier (TAII). This SAII-TAII pair defines a unique pseudowire between two PE devices.</p> <p>Auto-discovery routes are used by BGP to allow auto-discovery of SAIIs (the sources of the point-to-point pseudowires). One auto-discovery route is advertised for each source attachment identifier (SAI) in the instance or mesh group.</p> <p>The SAII is specified with the <b>source-attachment-identifier</b> statement within the FEC 129 VPWS routing instance. You configure the source attachment identifier and the interfaces to associate with that source attachment identifier. Under each interface, you can configure the TAII with the <b>target-attachment-identifier</b> statement. If the configured target identifier matches a source identifier advertised by a remote PE device by way of a BGP auto-discovery message, the pseudowire between that source-target pair is signaled. If there is no match between an advertised source identifier and the configured target identifier, the pseudowire is not established.</p> |
| <b>Options</b>                  | <p><b>identifier</b>—The numerical identifier for the Layer 2 VPN site.</p> <p><b>Range:</b> 1 through 4,292,967,295</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring FEC 129 BGP Autodiscovery for VPWS on page 708</a></li> <li>• <a href="#">source-attachment-identifier on page 1198</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## template

---

|                                 |                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | template;                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> protocols mpls label-switched-path <i>p2mp-lsp-template-name</i> ],<br>[edit protocols mpls label-switched-path <i>p2mp-lsp-template-name</i> ] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.3.<br>Statement introduced in Junos OS Release 12.3X50 for the QFX Series.                                                                            |
| <b>Description</b>              | Specify a template for the dynamically generated point-to-multipoint LSPs used for VPLS flooding.                                                                                                |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Dynamic Point-to-Multipoint Flooding LSPs with a Preconfigured Template on page 850</a></li></ul>                                |



## threshold (detection-time)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | threshold <i>milliseconds</i> ;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>     | <p>[edit logical-systems <i>logical-system-name</i> protocols bgp bfd-liveness-detection detection-time],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection detection-time],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection detection-time],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection detection-time],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection detection-time],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection detection-time],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection detection-time],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection detection-time],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection detection-time],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection detection-time],</p> <p>[edit protocols bgp bfd-liveness-detection detection-time],</p> <p>[edit protocols bgp group <i>group-name</i> bfd-liveness-detection detection-time],</p> <p>[edit protocols bgp group <i>group-name</i> neighbor <i>address</i> bgp bfd-liveness-detection detection-time],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection detection-time],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection detection-time],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection detection-time]</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection detection-time],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection detection-time],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection detection-time],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection detection-time]</p> |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 8.2.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for BFD authentication introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 13.2 for Layer 2 VPNs and VPLS.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Description** Specify the threshold for the adaptation of the BFD session detection time. When the detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.



**NOTE:** The threshold value must be equal to or greater than the transmit interval.

The threshold time must be equal to or greater than the value specified in the `minimum-interval` or the `minimum-receive-interval` statement.

**Options** *milliseconds*—Value for the detection time adaptation threshold.  
**Range:** 1 through 255,000

**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring BFD for Layer 2 VPN and VPLS on page 186](#)
- *Example: Configuring BFD for Static Routes*

## threshold (transmit-interval)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | threshold <i>milliseconds</i> ;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>     | <p>[edit logical-systems <i>logical-system-name</i> protocols bgp bfd-liveness-detection transmit-interval],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection transmit-interval],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection transmit-interval],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection transmit-interval],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection transmit-interval],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection transmit-interval],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection transmit-interval],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection transmit-interval],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection transmit-interval],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection transmit-interval],</p> <p>[edit protocols bgp bfd-liveness-detection transmit-interval],</p> <p>[edit protocols bgp group <i>group-name</i> bfd-liveness-detection transmit-interval],</p> <p>[edit protocols bgp group <i>group-name</i> neighbor <i>address</i> bgp bfd-liveness-detection transmit-interval],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection transmit-interval],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection transmit-interval],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection transmit-interval],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection transmit-interval],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection transmit-interval],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection transmit-interval],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection transmit-interval]</p> |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 8.2.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 12.1 for QFX Series.</p> <p>Statement introduced in Junos OS Release 13.2 for Layer 2 VPN and VPLS.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>         | Specify the threshold for the adaptation of the BFD session transmit interval. When the transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

**Options**    *milliseconds*—Value for the transmit interval adaptation threshold.

**Range:** 0 through 4,294,967,295 ( $2^{32} - 1$ )



**NOTE:** The threshold value specified in the `threshold` statement must be greater than the value specified in the `minimum-interval` statement for the `transmit-interval` statement.

---

**Required Privilege Level**    routing—To view this statement in the configuration.  
                                         routing-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring BFD for Layer 2 VPN and VPLS on page 186](#)
- *Example: Configuring BFD for Static Routes*
- *bfd-liveness-detection*

## traceoptions (Egress Protection)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;size <i>size</i>&gt; &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit protocols mpls egress-protection],                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.4R3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | Configure tracing operations for egress protection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Options</b>                  | <p><b><i>filename</i></b> —Name of the file to receive the output of the tracing operation.</p> <p><b><i>files number</i></b>—(Optional) Maximum number of trace files. If you specify a maximum number of files, you must also include the <b>size</b> statement to specify the maximum file size. When a trace file named <i>trace-file</i> reaches its maximum size, it is renamed <i>trace-file.0</i>, then <i>trace-file.1</i>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 2 files</p> <p><b><i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b><i>flag</i></b> statements.</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Trace all operations</li> <li>• <b>error</b>—Trace error conditions</li> <li>• <b>route</b>—Trace route transitions</li> <li>• <b>state</b>—Trace state transitions</li> </ul> |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Example: Configuring Egress Protection for Layer 3 VPN Services</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## traceoptions (Protocols EVPN)

---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre>traceoptions {<br/>    file <i>filename</i> &lt;files <i>number</i>&gt; &lt;size <i>size</i>&gt; &lt;world-readable   no-world-readable&gt;;<br/>    flag <i>flag</i> &lt;flag-modifier&gt;;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>     | [edit routing-instances <i>routing-instance-name</i> protocols evpn]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b> | Statement introduced in Junos OS Release 13.2 for MX 3D Series routers.<br>Statement introduced in Junos OS Release 14.2 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>         | Trace traffic flowing through an EVPN routing instance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Options</b>             | <p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" ").</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b><i>trace-file</i></b> reaches the maximum size as specified by the <b>size</b> option, it is renamed <b><i>trace-file.0</i></b>. When <b><i>trace-file</i></b> again reaches the maximum size, <b><i>trace-file.0</i></b> is renamed <b><i>trace-file.1</i></b> and <b><i>trace-file</i></b> is renamed <b><i>trace-file.0</i></b>. 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000 files</p> <p><b>Default:</b> 2 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can specify the following tracing flags:</p> <ul style="list-style-type: none"><li>• <b>all</b>—All EVPN tracing options</li><li>• <b>error</b>—Error conditions</li><li>• <b>general</b>—General events</li><li>• <b>mac-database</b>—MAC route database in the EVPN routing instance</li><li>• <b>nlri</b>—EVPN advertisements received or sent by means of BGP</li><li>• <b>normal</b>—Normal events</li><li>• <b>oam</b>—OAM messages</li><li>• <b>policy</b>—Policy processing</li><li>• <b>route</b>—Routing information</li><li>• <b>state</b>—State transitions</li><li>• <b>task</b>—Routing protocol task processing</li><li>• <b>timer</b>—Routing protocol timer processing</li></ul> |

- **topology**—EVPN topology changes caused by reconfiguration or advertisements received from other provider edge (PE) routers using BGP

**flag-modifier**—(Optional) Modifier for the tracing flag. You can specify the following modifiers:

- **detail**—Provide detailed trace information.
- **disable**—Disable this trace 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 the 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 (as specified by the **files** option) 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.

|                                 |                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Tracing EVPN Traffic and Operations on page 242</a></li> </ul> |

## traceoptions (Protocols Layer 2 Circuit)

---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre>traceoptions {<br/>    file <i>filename</i> &lt;files <i>number</i>&gt; &lt;size <i>size</i>&gt; &lt;world-readable   no-world-readable&gt;;<br/>    flag <i>flag</i> &lt;flag-modifier&gt; &lt;disable&gt;;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>     | [edit logical-systems <i>logical-system-name</i> protocols l2circuit],<br>[edit protocols l2circuit]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>         | Trace traffic flowing through a Layer 2 circuit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Options</b>             | <p><b>disable</b>—(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 <b>all</b>.</p> <p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" ").</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, and so on, 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000 files</p> <p><b>Default:</b> 2 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements.</p> <ul style="list-style-type: none"><li>• <b>connections</b>—Layer 2 circuit connections (events and state changes)</li><li>• <b>error</b>—Error conditions</li><li>• <b>fec</b>—Layer 2 circuit advertisements received or sent by means of LDP</li><li>• <b>topology</b>—Layer 2 circuit topology changes caused by reconfiguration or advertisements received from other PE routers</li></ul> <p><b>flag-modifier</b>—(Optional) Modifier for the tracing flag. You can specify the <b>detail</b> modifier if you want to provide detailed trace information.</p> <p><b>no-world-readable</b>—(Optional) Do not allow any user to read the log file.</p> <p><b>size <i>size</i></b>—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named <b>trace-file</b> reaches this size, it is renamed <b>trace-file.0</b>. When the <b>trace-file</b> again reaches its maximum size, <b>trace-file.0</b> is</p> |



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**—(Optional) Allow any user to read the log file.

|                           |                                                             |
|---------------------------|-------------------------------------------------------------|
| <b>Required Privilege</b> | routing—To view this statement in the configuration.        |
| <b>Level</b>              | routing-control—To add this statement to the configuration. |

|                              |                                                                                                                  |
|------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Related Documentation</b> | <ul style="list-style-type: none"><li>• <a href="#">Tracing Layer 2 Circuit Operations on page 443</a></li></ul> |
|------------------------------|------------------------------------------------------------------------------------------------------------------|

## traceoptions (Protocols Layer 2 VPN)

---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre>traceoptions {<br/>    file <i>filename</i> &lt;files <i>number</i>&gt; &lt;size <i>size</i>&gt; &lt;world-readable   no-world-readable&gt;;<br/>    flag <i>flag</i> &lt;<i>flag-modifier</i>&gt; &lt;disable&gt;;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>     | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn],<br>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b>         | Trace traffic flowing through a Layer 2 VPN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>             | <p><b>disable</b>—(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 <b>all</b>.</p> <p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" ").</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <i>trace-file</i> reaches its maximum size, it is renamed <i>trace-file.0</i>, then <i>trace-file.1</i>, and so on, 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000 files</p> <p><b>Default:</b> 2 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements.</p> <ul style="list-style-type: none"><li>• <b>all</b>—All Layer 2 VPN tracing options</li><li>• <b>connections</b>—Layer 2 connections (events and state changes)</li><li>• <b>error</b>—Error conditions</li><li>• <b>general</b>—General events</li><li>• <b>nlri</b>—Layer 2 advertisements received or sent by means of the BGP</li><li>• <b>normal</b>—Normal events</li><li>• <b>policy</b>—Policy processing</li><li>• <b>route</b>—Routing information</li><li>• <b>state</b>—State transitions</li><li>• <b>task</b>—Routing protocol task processing</li></ul> |

- **timer**—Routing protocol timer processing
- **topology**—Layer 2 VPN topology changes caused by reconfiguration or advertisements received from other PE routers using BGP

**flag-modifier**—(Optional) Modifier for the tracing flag. You can specify the following modifier:

- **detail**—Provide detailed trace information
- **receive**—Trace received packets
- **send**—Trace transmitted packets

**no-world-readable**—(Optional) Prevents any user from reading the trace 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**—(Optional) Allow any user to read the trace file.

**Default:** The default is **no-world-readable**.

|                                 |                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Tracing Layer 2 VPN Traffic and Operations on page 131</a></li> </ul> |

## traceoptions (Protocols VPLS)

---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre>traceoptions {<br/>    file <i>filename</i> &lt;files <i>number</i>&gt; &lt;size <i>size</i>&gt; &lt;world-readable   no-world-readable&gt;;<br/>    flag <i>flag</i> &lt;flag-modifier&gt; &lt;disable&gt;;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>     | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>         | Trace traffic flowing through a VPLS routing instance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>             | <p><b>disable</b>—(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 <b>all</b>.</p> <p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" ").</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches this size, it is renamed <b>trace-file.0</b>. When <b>trace-file</b> again reaches its maximum size, <b>trace-file.0</b> is renamed <b>trace-file.1</b> and <b>trace-file</b> is renamed <b>trace-file.0</b>. 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000 files</p> <p><b>Default:</b> 2 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can specify the following tracing flags:</p> <ul style="list-style-type: none"><li>• <b>all</b>—All VPLS tracing options</li><li>• <b>connections</b>—VPLS connections (events and state changes)</li><li>• <b>error</b>—Error conditions</li><li>• <b>nlri</b>—VPLS advertisements received or sent by means of the BGP</li><li>• <b>route</b>—Routing information</li><li>• <b>topology</b>—VPLS topology changes caused by reconfiguration or advertisements received from other provider edge (PE) routers using BGP</li></ul> <p><b>flag-modifier</b>—(Optional) Modifier for the tracing flag. You can specify the following modifiers:</p> <ul style="list-style-type: none"><li>• <b>detail</b>—Provide detailed trace information.</li></ul> |

- **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.

|                                 |                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Tracing VPLS Traffic and Operations on page 940</a></li> </ul> |

## transmit-interval (BFD Liveness Detection)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre>transmit-interval {     minimum-interval milliseconds;     threshold milliseconds; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>     | <pre>[edit logical-systems <i>logical-system-name</i> protocols bgp bfd-liveness-detection], [edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i>   bfd-liveness-detection], [edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i>   bfd-liveness-detection], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   bgp bfd-liveness-detection], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   bgp group <i>group-name</i> bfd-liveness-detection], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection], [edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   l2vpn oam bfd-liveness-detection], [edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection], [edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection], [edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols   vpls oam bfd-liveness-detection], [edit protocols bgp bfd-liveness-detection], [edit protocols bgp group <i>group-name</i> bfd-liveness-detection], [edit protocols bgp group <i>group-name</i> neighbor <i>address</i> bgp bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i>   bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor   <i>address</i> bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam   bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>   neighbor <i>neighbor-id</i> oam bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection]</pre> |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 8.2.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for BFD authentication introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 13.2 for Layer 2 VPN and VPLS.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>         | <p>Specify the transmit interval for the <b>bfd-liveness-detection</b> statement. The negotiated transmit interval for a peer is the interval between the sending of BFD packets to peers. The receive interval for a peer is the minimum time that it requires between packets sent from its peer; the receive interval is not negotiated between peers. To determine the transmit interval, each peer compares its configured minimum transmit interval with its</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |


peer's minimum receive interval. The larger of the two numbers is accepted as the transmit interval for that peer.

The remaining statements are explained separately.

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring BFD for Layer 2 VPN and VPLS on page 186</a></li><li>• <i>Example: Configuring BFD for Static Routes</i></li><li>• <i>bfd-liveness-detection</i></li><li>• <a href="#">threshold on page 1207</a></li><li>• <a href="#">minimum-interval on page 1148</a></li><li>• <a href="#">minimum-receive-interval on page 1150</a></li></ul> |

## tunnel-services (Routing Instances VPLS)

---

|                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                 | <pre>tunnel-services {<br/>    devices <i>device-names</i>;<br/>    primary <i>primary-device-name</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                        | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls],<br>[edit routing-instances <i>routing-instance-name</i> protocols vpls]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>                                                                                                                                                                                                                                    | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>                                                                                                                                                                                                                                            | Specify that traffic for particular VPLS routing instances be forwarded to specific virtual tunnel (VT) interfaces, allowing you to load-balance VPLS traffic among all the available VT interfaces on the router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <div> <b>NOTE:</b> In the VPLS documentation, the word <i>router</i> in terms such as <i>PE router</i> is used to refer to any device that provides routing functions.</div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>                                                                                                                                                                                                                                                | <p><b>devices <i>device-names</i></b>—Specify the VT interfaces acceptable for use by the VPLS routing instance. If you do not configure this option, all VT interfaces available to the router can be used for de-encapsulating traffic for this instance.</p> <p><b>primary <i>primary-device-name</i></b>—Specify the primary VT interface to be used by the VPLS routing instance. The VT interface specified is used to de-encapsulate all VPLS traffic from the MPLS core network for this routing instance. If the VT interface specified is unavailable, then one of the other acceptable VT interfaces is used for handling the VPLS traffic. If you do not configure this option, any acceptable VT interface can be used to de-encapsulate VPLS traffic from the core.</p> |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                               | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>                                                                                                                                                                                                                                  | <ul style="list-style-type: none"><li>• <a href="#">Specifying the VT Interfaces Used by VPLS Routing Instances on page 579</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



## version (BFD Liveness Detection)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | version (0   1   automatic);                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>     | <p>[edit logical-systems <i>logical-system-name</i> protocols bgp bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit logical-system <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection],</p> <p>[edit protocols bgp bfd-liveness-detection],</p> <p>[edit protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit protocols bgp group <i>group-name</i> neighbor <i>address</i> bgp bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols bgp group <i>group-name</i> neighbor <i>address</i> bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn oam bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> oam bfd-liveness-detection],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls oam bfd-liveness-detection]</p> |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 8.1</p> <p>Statement introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 13.2 for Layer 2 VPN and VPLS.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>         | Specify the BFD version for detection. You can explicitly configure BFD version 0, version 1, or the routing device can automatically detect the BFD version. By default, the routing device automatically detects the BFD version, which is either 0 or 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Options</b>             | Configure the BFD version to detect: <b>0</b> (BFD version 0), <b>1</b> (BFD version 1), or <b>automatic</b> (autodetect the BFD version)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                            | <b>Default:</b> automatic                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring BFD for Layer 2 VPN and VPLS on page 186](#)
- [Example: Configuring BFD Authentication for BGP](#)
- [Example: Configuring BFD on Internal BGP Peer Sessions](#)
- [Example: Configuring BFD Authentication for BGP](#)
- [Understanding BFD Authentication for BGP](#)

---

## virtual-circuit-id

---

**Syntax** virtual-circuit-id *identifier*;

**Hierarchy Level** [edit logical-systems *logical-system-name* protocols l2circuit local-switching interface *interface-name* backup-neighbor *address*],  
[edit logical-systems *logical-system-name* protocols l2circuit neighbor *address* interface *interface-name*],  
[edit logical-systems *logical-system-name* protocols l2circuit neighbor *address* interface *interface-name* backup-neighbor *address*],  
[edit protocols l2circuit local-switching interface *interface-name* backup-neighbor *address*],  
[edit protocols l2circuit neighbor *address* interface *interface-name*],  
[edit protocols l2circuit neighbor *address* interface *interface-name* backup-neighbor *address*]

**Release Information** Statement introduced before Junos OS Release 7.4.  
Hierarchy levels for **backup-neighbor** (pseudowire redundancy) added in Junos OS Release 9.2.  
Statement introduced in Junos OS Release 11.1 for EX Series switches.  
Statement introduced in Junos OS Release 12.3 at the [edit protocols l2circuit local-switching interface *interface-name* backup-neighbor *address*] hierarchy level.

**Description** Uniquely identify a Layer 2 circuit for either a standard pseudowire or a redundant pseudowire.

**Options** *identifier*—1 through 4,294,967,295

**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring the Virtual Circuit ID on page 356](#)
- [Configuring Pseudowire Redundancy on the PE Router on page 180](#)
- [Example: Configuring Layer 2 Circuit Switching Protection on page 420](#)

## virtual-mac

|                                 |                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>virtual-mac <i>mac-address/mask</i>;</code>                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit protocols l2-learning vpls-mac-move]                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 14.2.                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Configure MAC addresses that are not to be considered in the VPLS loop prevention algorithm.                                                                                                                                                                                                          |
| <b>Options</b>                  | <p><i>mac-address/mask</i>— MAC address</p> <p><b>Values:</b> 00:00:5e:00:01:00/8, 00:00:0c:07:ac:00/8, and 02:bf:00:00:00:00/32</p>                                                                                                                                                                  |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">MAC Moves Loop Prevention in VPLS Network Overview on page 900</a></li> <li>• <a href="#">Example: Configuring Loop Prevention in VPLS Network Due to MAC Moves on page 903</a></li> <li>• <a href="#">vpls-mac-move on page 1231</a></li> </ul> |

## vlan-id

|                                 |                                                                                                                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>vlan-id <i>number</i>;</code>                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</p>                                               |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                       |
| <b>Description</b>              | For Fast Ethernet and Gigabit Ethernet interfaces only, bind an 802.1Q VLAN tag ID to a logical interface.                                                                                                                                              |
| <b>Options</b>                  | <p><i>number</i>—A valid VLAN identifier.</p> <p><b>Range:</b> For 4-port Fast Ethernet PICs configured to handle VPLS traffic, 512 through 1023. For 1-port and 10-port Gigabit Ethernet PICs configured to handle VPLS traffic, 512 through 4094.</p> |
| <b>Required Privilege Level</b> | <p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Interfaces for VPLS Routing on page 603</a></li> </ul>                                                                                                                                 |

## vlan-id (routing instance)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>vlan-id (vlan-id   all   none);</code>                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> ],<br>[edit routing-instances <i>routing-instance-name</i> ]                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2.<br>Statement introduced in Junos OS Release 14.2 for EX Series switches.                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Specify 802.1Q VLAN tag IDs to a routing instance.                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                  | <p><b>vlan-id</b>—A valid VLAN identifier.</p> <p><b>Range:</b> For 4-port Fast Ethernet PICs, 512 through 1023. For 1-port and 10-port Gigabit Ethernet PICs configured to handle VPLS traffic, 512 through 4094.</p> <p><b>all</b>—Include all VLAN identifiers specified on the logical interfaces included in the routing instance.</p> <p><b>none</b>—Include no VLAN identifiers for the routing instance.</p> |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring EVPN Routing Instances on page 239</a></li><li>• <a href="#">Configuring EVPN Routing Instances on EX9200 Switches</a></li></ul>                                                                                                                                                                                                                     |

## vlan-id-list (Interface in VPLS)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>vlan-id-list [ <i>numbers number-number</i> ];</code>                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ],<br>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced for VPLS in Junos OS Release 10.2.                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | Configure a logical interface to forward packets and learn MAC addresses within each VPLS routing instance configured with a VLAN ID that matches a VLAN ID specified in the list. VLAN IDs can be entered individually using a space to separate each ID, entered as an inclusive list separating the starting VLAN ID and ending VLAN ID with a hyphen, or a combination of both. |
| <b>Options</b>                  | <p><i>number number</i>—Individual VLAN IDs separated by a space.</p> <p><i>number-number</i>—Starting VLAN ID and ending VLAN ID in an inclusive range.</p> <p><b>Range:</b> 1 through 4095</p>                                                                                                                                                                                    |
| <b>Required Privilege Level</b> | <p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Interfaces for VPLS Routing on page 603</a></li> <li>• <a href="#">Configuring VLAN IDs for Logical Interfaces on page 607</a></li> </ul>                                                                                                                                                                          |

## vlan-tagging

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | vlan-tagging;                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> ]                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.<br>Statement introduced in Junos OS Release 13.2 for PTX Series Routers.<br>Statement introduced in Junos OS Release 14.1X53-D10 for the QFX Series.                               |
| <b>Description</b>              | For Fast Ethernet and Gigabit Ethernet interfaces and aggregated Ethernet interfaces configured for VPLS, enable the reception and transmission of 802.1Q VLAN-tagged frames on the interface.                                                                                                                                                                                                         |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">802.1Q VLANs Overview</a></li><li>• <a href="#">vlan-id</a></li><li>• <a href="#">Configuring a Layer 3 Subinterface (CLI Procedure)</a></li><li>• <a href="#">Configuring Tagged Aggregated Ethernet Interfaces</a></li><li>• <a href="#">Example: Configuring Layer 3 Subinterfaces for a Distribution Switch and an Access Switch</a></li></ul> |

## vpls (Interfaces)

---

|                                 |                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | vpls;                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family],<br>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                            |
| <b>Description</b>              | Specify the VPLS protocol family information for the logical interface.                                                                                                                                      |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Interfaces for VPLS Routing on page 603</a></li></ul>                                                                                        |

## vpls (Routing Instance)

```
Syntax vpls {
 active-interface {
 any;
 primary interface-name;
 }
 community COMM;
 connectivity-type (ce | irb);
 control-word;
 encapsulation-type ethernet;
 ignore-encapsulation-mismatch;
 ignore-mtu-mismatch;
 interface interface-name;
 interface-mac-limit limit;
 label-block-size size;
 mac-flush [explicit-mac-flush-message-options];
 mac-table-aging-time time;
 mac-table-size size;
 mesh-group mesh-group-name {
 l2vpn-id (as-number:id | ip-address:id);
 local-switching;
 mac-flush [explicit-mac-flush-message-options];
 neighbor address {...}
 peer-as all;
 pseudowire-status-tlv;
 route-distinguisher (as-number:id | ip-address:id);
 vpls-id number;
 vrf-export [policy-names];
 vrf-import [policy-names];
 vrf-target {
 community;
 import community-name;
 export community-name;
 }
 }
 mtu mtu;
 no-control-word;
 no-tunnel-services;
 site site-name {
 active-interface interface-name {
 any;
 primary preference-value;
 }
 best-site;
 interface interface-name {
 interface-mac-limit limit;
 }
 mesh-group mesh-group-name;
 multi-homing;
 site-identifier identifier;
 site-preference preference-value {
 backup;
 primary;
 }
 }
}
```

```
 }
 }
 site-range number;
 traceoptions {
 file filename <files number> <size size> <world-readable | no-world-readable>;
 flag flag <flag-modifier> <disable>;
 }
 tunnel-services {
 devices device-names;
 primary primary-device-name;
 }
}
```

|                          |                                                                                                                                                                                |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hierarchy Level          | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols],<br>[edit routing-instances <i>routing-instance-name</i> protocols] |
| Release Information      | Statement introduced before Junos OS Release 7.4. The <b>mac-flush</b> option was added in Junos OS Release 10.0.                                                              |
| Description              | Configure a virtual private LAN service (VPLS) routing instance.<br><br>The remaining statements are explained separately.                                                     |
| Required Privilege Level | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                            |
| Related Documentation    | <ul style="list-style-type: none"><li>• <a href="#">Configuring VPLS Routing Instances on page 563</a></li></ul>                                                               |



## vpls-id

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>vpls-id <i>vpls-id</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols l2vpn],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols l2vpn mesh-group <i>mesh-group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>],</p> <p>[edit routing-instances <i>instance-name</i> protocols l2vpn],</p> <p>[edit routing-instances <i>instance-name</i> protocols l2vpn mesh-group <i>mesh-group-name</i>],</p> <p>[edit routing-instances <i>instance-name</i> protocols vpls],</p> <p>[edit routing-instances <i>instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>]</p> |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | Identify the virtual circuit identifier used for the VPLS routing instance or mesh group. This statement is a part of the configuration to enable LDP signaling for VPLS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Options</b>                  | <i>vpls-id</i> —Specify a valid identifier for the VPLS routing instance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring LDP Signaling for VPLS on page 569</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## vpls-id-list (protocols vpls mesh-group)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>vpls-id-list <i>vc-id-numbers</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>address</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 14.2 for MX Series routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | <p>The <b>vpls-id-list</b> option allows you to configure multiple pseudowires under LDP-VPLS neighbor by creating one pseudowire per virtual circuit id. This combination of neighbor and virtual circuit ID must be unique across the l2circuit and all local LDP-VPLS instances. The pseudowire will terminate in the specified mesh-group.</p> <p>As with other pseudowires, the pseudowires created here will signal the remote PE via LDP label mapping message. For each pseudowire created under a neighbor, VPLS will create a VT/LSI interface and add both it and the and label route to the mpls.0 table. Note that you can create multiple pseudowires between the same pair of PEs in LDP-VPLS for a single routing instances only.</p> <p>Enable <b>local-switching</b> along with <b>vpls-id-list</b> to allow local switching of traffic (including BUM traffic) between multiple pseudo wires. This can also eliminate the need to have a dedicated mesh-group for each LDP spoke pseudo wire (which has a limit of 14), and provide support for H-VPLS in EVP-LAN and EP-LAN topologies.</p> |
| <b>Options</b>                  | <b><i>vc-id-numbers</i></b> —The virtual circuit ID for the PE pair. This ID can be any number in the range of 1 to 4294967295.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show vpls connections on page 1305</a></li><li>• <a href="#">neighbor on page 1161</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## vpls-mac-move

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>vpls-mac-move {   cooloff-time <i>seconds</i>;   interface-recovery-time <i>seconds</i>;   statistical-approach-wait-time <i>seconds</i>;   virtual-mac <i>mac-address</i> /<i>mask</i>; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit protocols l2-learning]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 14.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | Configure VPLS MAC move parameters to prevent loop creation in the network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Options</b>                  | <p><b>cooloff-time <i>seconds</i></b>— Time interval, in seconds, during which no additional interface is disabled by the PE after a MAC move is detected. By default, it is 30 seconds.</p> <p><b>interface-recovery-time <i>seconds</i></b>— Time interval, in seconds, after which the interface is enabled after a VPLS MAC move is detected. By default, the timer is disabled.</p> <p><b>statistical-approach-wait-time <i>seconds</i></b>— Time interval, in seconds, during which the MAC moves are monitored to collect the statistics. By default, it is 30 seconds.</p> <p>The remaining statement is explained separately.</p> |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">MAC Moves Loop Prevention in VPLS Network Overview on page 900</a></li> <li>• <a href="#">Example: Configuring Loop Prevention in VPLS Network Due to MAC Moves on page 904</a></li> <li>• <a href="#">virtual-mac on page 1223</a></li> </ul>                                                                                                                                                                                                                                                                                                                                        |



## CHAPTER 48

# Operational Commands

- clear pim snooping join
- clear pim snooping statistics
- clear security group-vpn member ike security-associations
- clear security group-vpn member kek security-associations
- clear vpls mac-address
- clear vpls mac-move-action
- clear vpls mac-table
- ping mpls l2circuit
- ping mpls l2vpn
- ping vpls instance
- request l2circuit-switchover
- show evpn instance
- show interfaces lsi (Label-Switched Interface)
- show l2circuit connections
- show l2vpn connections
- show pim snooping interfaces
- show pim snooping join
- show pim snooping neighbors
- show pim snooping statistics
- show route
- show security group-vpn member ike security-associations
- show security group-vpn member kek security-associations
- show vpls connections
- show vpls flood event-queue
- show vpls flood instance
- show vpls flood route
- show vpls mac-move-action

- [show vpls mac-table](#)
- [show vpls statistics](#)

## clear pim snooping join

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear pim snooping join<br><instance <i>instance-name</i> ><br><logical-system <i>logical-system-name</i> ><br><vlan-id <i>vlan-id</i> >                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Command introduced in Junos OS Release 12.3 for MX Series 3D Universal Edge devices.<br>Command introduced in Junos OS Release 13.2 for M Series Multiservice Edge devices.                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | Clear information about Protocol Independent Multicast (PIM) snooping joins.                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Options</b>                  | <p><b>none</b>—Display detailed information.</p> <p><b>instance <i>instance-name</i></b>—(Optional) Clear PIM snooping join information for the specified routing instance.</p> <p><b>logical-system <i>logical-system-name</i></b>—(Optional) Delete the IGMP snooping statistics for a given logical system or for all logical systems.</p> <p><b>vlan-id <i>vlan-identifier</i></b>—(Optional) Clear PIM snooping join information for the specified VLAN.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>PIM Snooping for VPLS</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>List of Sample Output</b>    | <a href="#">clear pim snooping join on page 1235</a>                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Output Fields</b>            | See <a href="#">show pim snooping join</a> for an explanation of the output fields.                                                                                                                                                                                                                                                                                                                                                                               |

## Sample Output

### clear pim snooping join

The following sample output displays information about PIM snooping joins before and after the **clear pim snooping join** command is entered:

```

user@host> show pim snooping join extensive
Instance: vpls1
Learning-Domain: vlan-id 10
Learning-Domain: vlan-id 20

Group: 198.51.100.2
Source: *
Flags: sparse,rptree,wildcard
Upstream state: None
Upstream neighbor: 192.0.2.5, port: ge-1/3/7.20
Downstream port: ge-1/3/1.20
Downstream neighbors:
192.0.2.2 State: Join Flags: SRW Timeout: 185

Group: 198.51.100.3

```

```
Source: *
Flags: sparse,rptree,wildcard
Upstream state: None
Upstream neighbor: 192.0.2.4, port: ge-1/3/5.20
Downstream port: ge-1/3/3.20
Downstream neighbors:
192.0.2.3 State: Join Flags: SRW Timeout: 175

user@host> clear pim snooping join
Clearing the Join/Prune state for 224.0.0.0/4
Clearing the Join/Prune state for 224.0.0.0/4

user@host> show pim snooping join extensive
Instance: vpls1
Learning-Domain: vlan-id 10
Learning-Domain: vlan-id 20
```



## clear pim snooping statistics

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear pim snooping statistics<br><instance <i>instance-name</i> ><br><interface <i>interface-name</i> ><br><logical-system <i>logical-system-name</i> ><br><vlan-id <i>vlan-id</i> >                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Command introduced in Junos OS Release 12.3 for MX Series 3D Universal Edge devices.<br>Command introduced in Junos OS Release 13.2 for M Series Multiservice Edge devices.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | Clear Protocol Independent Multicast (PIM) snooping statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <p><b>none</b>—Clear PIM snooping statistics for all family addresses, instances, and interfaces.</p> <p><b>instance <i>instance-name</i></b>—(Optional) Clear statistics for a specific PIM-snooping-enabled routing instance.</p> <p><b>interface <i>interface-name</i></b>—(Optional) Clear PIM snooping statistics for a specific interface.</p> <p><b>logical-system <i>logical-system-name</i></b>—(Optional) Delete the IGMP snooping statistics for a given logical system or for all logical systems.</p> <p><b>vlan-id <i>vlan-identifier</i></b>—(Optional) Clear PIM snooping statistics information for the specified VLAN.</p> |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>PIM Snooping for VPLS</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>List of Sample Output</b>    | <a href="#">clear pim snooping statistics on page 1237</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Output Fields</b>            | See <a href="#">show pim snooping statistics</a> for an explanation of the output fields.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Sample Output

### clear pim snooping statistics

The following sample output displays PIM snooping statistics before and after the **clear pim snooping statistics** command is entered:

```
user@host> show pim snooping statistics
Instance: vpls1
Learning-Domain: vlan-id 10

Tx J/P messages 0
RX J/P messages 660
Rx J/P messages -- seen 0
Rx J/P messages -- received 660
Rx Hello messages 1396
Rx Version Unknown 0
Rx Neighbor Unknown 0
```

```
Rx Upstream Neighbor Unknown 0
Rx Bad Length 0
Rx J/P Busy Drop 0
Rx J/P Group Aggregate 0
Rx Malformed Packet 0

Learning-Domain: vlan-id 20

user@host> clear pim snooping statistics
user@host> show pim snooping statistics
Instance: vpls1
Learning-Domain: vlan-id 10

Tx J/P messages 0
RX J/P messages 0
Rx J/P messages -- seen 0
Rx J/P messages -- received 0
Rx Hello messages 0
Rx Version Unknown 0
Rx Neighbor Unknown 0
Rx Upstream Neighbor Unknown 0
Rx Bad Length 0
Rx J/P Busy Drop 0
Rx J/P Group Aggregate 0
Rx Malformed Packet 0

Learning-Domain: vlan-id 20
```

## **clear security group-vpn member ike security-associations**

---

|                                 |                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear security group-vpn member ike security-associations [ <i>index SA-index</i> ] [ <i>peer-ipaddress</i> ]                                                                                                                                         |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.2.                                                                                                                                                                                                          |
| <b>Description</b>              | Clear IKE security association (SA) for a group member.                                                                                                                                                                                               |
| <b>Options</b>                  | <ul style="list-style-type: none"><li>• none—Clear all IKE SAs for the group member.</li><li>• <i>index</i>—(Optional) Clear the IKE SA with this index number.</li><li>• <i>peer-ipaddress</i>—(Optional) Clear the IKE SA with this peer.</li></ul> |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show security group-vpn member ike security-associations on page 1298</a></li><li>• <i>Group VPNv2 Overview</i></li></ul>                                                                         |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                                      |

## [clear security group-vpn member kek security-associations](#)

---

|                                 |                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear security group-vpn member kek security-associations [index <i>SA-index</i> ]                                                                                            |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.2.                                                                                                                                  |
| <b>Description</b>              | Clear key encryption key (KEK) SAs for a group member.                                                                                                                        |
| <b>Options</b>                  | <ul style="list-style-type: none"><li>• none—Clear all KEK SAs for the group member.</li><li>• index—(Optional) Clear the KEK SA with this index number.</li></ul>            |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show security group-vpn member kek security-associations on page 1301</a></li><li>• <i>Group VPNv2 Overview</i></li></ul> |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                              |

## clear vpls mac-address

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear vpls mac-address<br><instance <i>instance-name</i> ><br><logical-system (all   <i>logical-system-name</i> )><br><mac-address>                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | (T Series and M Series routers, except for the M160 router) Clear media access control (MAC) address entries from the virtual private LAN service (VPLS) table.                                                                                                                                                                                                                                                                                                                                     |
| <b>Options</b>                  | <p><b>none</b>—Clear all MAC address entries from the VPLS table for all routing instances.</p> <p><b>instance <i>instance-name</i></b>—(Optional) Clear all MAC address entries for a VPLS instance from the VPLS table.</p> <p><b>logical-system (all   <i>logical-system-name</i>)</b>—(Optional) Perform this operation on all logical systems or on a particular logical system.</p> <p><b>mac-address</b>—(Optional) Clear a specific MAC address in a VPLS instance from the VPLS table.</p> |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>List of Sample Output</b>    | <a href="#">clear vpls mac-address on page 1241</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                                                                                                                                                                                                                                                                                               |

### Sample Output

#### clear vpls mac-address

```
user@host> clear vpls mac-address
```

## clear vpls mac-move-action

---

|                                 |                                                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>clear vpls mac-move-action</code><br><code>&lt;interface ifl-name.unit&gt;</code>                                                                            |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.2.                                                                                                                       |
| <b>Description</b>              | Clear the learning interfaces (IFLs) disabled due to a MAC move.                                                                                                   |
| <b>Options</b>                  | <b>none</b> —Clear all the IFLs disabled due to a MAC move.<br><br><b>interface ifl-name.unit</b> —(Optional) Clear the VPLS interface disabled due to a MAC move. |
| <b>Required Privilege Level</b> | clear                                                                                                                                                              |
| <b>List of Sample Output</b>    | <a href="#">clear vpls mac-move-action (MX Series) on page 1242</a><br><a href="#">clear vpls mac-move-action interface ifl-name.unit (MX Series) on page 1242</a> |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                              |

### Sample Output

#### clear vpls mac-move-action (MX Series)

```
user@host> clear vpls mac-move-action
```

#### clear vpls mac-move-action interface ifl-name.unit (MX Series)

```
user@host> clear vpls mac-move-action interface xe-1/0/0.1
```

## clear vpls mac-table

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear vpls mac-table<br><instance <i>instance-name</i> ><br><interface <i>interface-name</i> ><br><logical-system (all   <i>logical-system-name</i> )><br><mac-address><br><vlan-id>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Command introduced before Junos OS Release 9.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>              | (MX Series routers) Clear media access control (MAC) addresses from the virtual private LAN service (VPLS) MAC table.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Options</b>                  | <p><b>none</b>—Clear all MAC addresses from the VPLS table for all routing instances.</p> <p><b>instance <i>instance-name</i></b>—(Optional) Clear all MAC addresses for a VPLS instance from the VPLS table.</p> <p><b>interface <i>interface-name</i></b>—(Optional) Clear all MAC addresses for a VPLS interface from the VPLS table.</p> <p><b>logical-system (all   <i>logical-system-name</i>)</b>—(Optional) Perform this operation on all logical systems or on a particular logical system.</p> <p><b>mac-address</b>—(Optional) Clear a specific MAC address in a VPLS instance from the VPLS table.</p> <p><b>vlan-id</b>—(Optional) Clear MAC addresses on a specified VLAN (0 through 4095).</p> |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>List of Sample Output</b>    | <a href="#">clear vpls mac-table on page 1243</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Sample Output

### clear vpls mac-table

```
user@host> clear vpls mac-table
```

## ping mpls l2circuit

---

**Syntax** ping mpls l2circuit (interface *interface-name* | virtual-circuit *virtual-circuit-id* neighbor *address*)  
<count *count*>  
<destination *address*>  
<detail>  
<exp *forwarding-class*>  
<logical-system (all | *logical-system-name*)>  
reply-mode (application-level-control-channel | ip-udp | no-reply)  
<size *bytes*>  
<source *source-address*>  
<sweep>  
<v1>

**Release Information** Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 12.3X50 for the QFX Series.  
The **size** and **sweep** options were introduced in Junos OS Release 9.6.  
The **reply-mode** option and its suboptions are introduced in Junos OS Release 10.4R1.

**Description** Check the operability of the MPLS Layer 2 circuit connections. Type Ctrl+c to interrupt a ping mpls l2circuit command.

**Options** **count** *count*—(Optional) Number of ping requests to send. If **count** is not specified, five ping requests are sent. The range of values is 1 through 1,000,000. The default value is 5.

**destination** *address*—(Optional) Specify an address other than the default (127.0.0.1/32) for the ping echo requests. The address can be anything within the 127/8 subnet.

**detail**—(Optional) Display detailed information about the echo requests sent and received.

**exp** *forwarding-class*—(Optional) Value of the forwarding class for the MPLS ping packets.

**interface** *interface-name*—Ping an interface configured for the Layer 2 circuit on the egress provider edge (PE) router.

**logical-system** (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on the specified logical system.

**reply-mode**—(Optional) Reply mode for the ping request. This option has the following suboptions:

**application-level-control-channel**—Reply using an application level control channel.

**ip-udp**—Reply using an IPv4 or IPv6 UDP packet.

**no-reply**—Do not reply to the ping request.





**NOTE:** The **reply-mode** option and its suboptions **application-level-control-channel**, **ip-udp**, and **no-reply** are also available in Junos OS Release 10.2R4 and 10.3R2.

**size bytes**—(Optional) Size of the label-switched path (LSP) ping request packet (96 through 65468 bytes). Packets are 4-byte aligned. For example, If you enter a size of 97, 98, 99, or 100, the router or switch uses a size value of 100 bytes. If you enter a packet size that is smaller than the minimum size, an error message is displayed reminding you of the 96-byte minimum.

**source source-address**—(Optional) IP address of the outgoing interface. This address is sent in the IP source address field of the ping request. If this option is not specified, the default address is usually the loopback interface (**lo.0**).

**sweep**—(Optional) Automatically determine the size of the maximum transmission unit (MTU).

**vtl**—(Optional) Use the type 9 Layer 2 circuit type, length, and value (TLV).

**virtual-circuit virtual-circuit-id neighbor address**—Ping the virtual circuit identifier on the egress PE router or switch and the specified neighbor, testing the integrity of the Layer 2 circuit between the ingress and egress PE routers or switches.

**Additional Information** You must configure MPLS at the **[edit protocols mpls]** hierarchy level on the egress PE router or switch (the router or switch receiving the MPLS echo packets) to ping a Layer 2 circuit.

In asymmetric MTU scenarios, the echo response might be dropped. For example, if the MTU from System A to System B is 1000 bytes, the MTU from System B to System A is 500 bytes, and the ping request packet size is 1000 bytes, the echo response is dropped because the PAD TLV is included in the echo response, making it too large.

**Required Privilege Level** network

**List of Sample Output** [ping mpls l2circuit interface on page 1246](#)  
[ping mpls l2circuit virtual-circuit detail on page 1246](#)  
[ping mpls l2circuit interface <interface-name> reply-mode on page 1246](#)

**Output Fields** When you enter this command, you are provided feedback on the status of your request. An exclamation point (!) indicates that an echo reply was received. A period (.) indicates that an echo reply was not received within the timeout period. An x indicates that an echo reply was received with an error code. Packets with an error code are not counted in the received packets count. They are accounted for separately.

## Sample Output

### ping mpls l2circuit interface

```
user@host> ping mpls l2circuit interface so-1/0/0.1
Request for seq 1, to interface 69, labels <100000, 100208>, packet size 100
Reply for seq 1, return code: Egress-ok, time: 0.439 ms
```

### ping mpls l2circuit virtual-circuit detail

```
user@host> ping mpls l2circuit virtual-circuit 200 neighbor 10.255.245.122/32 detail
Request for seq 1, to interface 68, labels <100048, 100128>, packet size 100

Reply for seq 1, return code: Egress-ok time: 0.539 ms
```

### ping mpls l2circuit interface <interface-name> reply-mode

```
user@host> ping mpls l2circuit interface lt-1/2/0.21 reply-mode application-level-control-channel
!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

## ping mpls l2vpn

**Syntax** ping mpls l2vpn (instance *instance-name* local-site-id *local-site-id-number* remote-site-id *remote-site-id-number* | interface *interface-name*)  
 <bottom-label-ttl>  
 <count *count*>  
 <destination *address*>  
 <detail>  
 <exp *forwarding-class*>  
 <logical-system (all | *logical-system-name*)>  
 reply-mode (application-level-control-channel | ip-udp | no-reply)  
 <size *bytes*>  
 <source *source-address*>  
 <sweep>

**Release Information** Command introduced before Junos OS Release 7.4.  
 Command introduced in Junos OS Release 9.0 for EX Series switches.  
 The **size** and **sweep** options were introduced in Junos OS Release 9.6.  
 The **reply-mode** option and its suboptions are introduced in Junos OS Release 10.4R1.

**Description** Check the operability of MPLS Layer 2 virtual private network (VPN) connections. Type Ctrl+c to interrupt a **ping mpls l2vpn** command.

**Options** **bottom-label-ttl**—(Optional) Display the time-to-live value for the bottom label in the label stack.

**count** *count*—(Optional) Number of ping requests to send. If **count** is not specified, five ping requests are sent. The range of values is 1 through 1,000,000. The default value is 5.

**destination** *address*—(Optional) Specify an address other than the default (127.0.0.1/32) for the ping echo requests. The address can be anything within the 127/8 subnet.

**detail**—(Optional) Display detailed information about the echo requests sent and received.

**exp** *forwarding-class*—(Optional) Value of the forwarding class for the MPLS ping packets.

**instance** *instance-name* local-site-id *local-site-id-number* remote-site-id *remote-site-id-number*—Ping a combination of the Layer 2 VPN routing instance name, the local site identifier, and the remote site identifier, testing the integrity of the Layer 2 VPN circuit (specified by the identifiers) between the ingress and egress provider edge (PE) routers or switches.

**interface** *interface-name*—Ping an interface configured for the Layer 2 VPN on the egress PE router or switch.

**logical-system** (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on the specified logical system.

**reply-mode**—(Optional) Reply mode for the ping request. This option has the following suboptions:

**application-level-control-channel**—Reply using an application level control channel.

**ip-udp**—Reply using an IPv4 or IPv6 UDP packet.

**no-reply**—Do not reply to the ping request.

The **reply-mode** option and its suboptions **application-level-control-channel**, **ip-udp**, and **no-reply** are also available in Junos OS Release 10.2R4 and 10.3R2.

**size bytes**—(Optional) Size of the label-switched path (LSP) ping request packet (96 through 65468 bytes). Packets are 4-byte aligned. For example, If you enter a size of 97, 98, 99, or 100, the router or switch uses a size value of 100 bytes. If you enter a packet size that is smaller than the minimum size, an error message is displayed reminding you of the 96-byte minimum.

**source source-address**—(Optional) IP address of the outgoing interface. This address is sent in the IP source address field of the ping request. If this option is not specified, the default address is usually the loopback interface (**lo.0**).

**sweep**—(Optional) Automatically determine the size of the maximum transmission unit (MTU).

#### Additional Information

You must configure MPLS at the **[edit protocols mpls]** hierarchy level on the egress PE router or switch (the router or switch receiving the MPLS echo packets) to ping a Layer 2 circuit.

In asymmetric MTU scenarios, the echo response might be dropped. For example, if the MTU from System A to System B is 1000 bytes, the MTU from System B to System A is 500 bytes, and the ping request packet size is 1000 bytes, the echo response is dropped because the PAD TLV is included in the echo response, making it too large.

#### Required Privilege Level

network

#### List of Sample Output

[ping mpls l2vpn instance on page 1248](#)  
[ping mpls l2vpn instance detail on page 1249](#)  
[ping mpls l2vpn interface <interface-name> reply-mode on page 1249](#)

#### Output Fields

When you enter this command, you are provided feedback on the status of your request. An exclamation point (!) indicates that an echo reply was received. A period (.) indicates that an echo reply was not received within the timeout period. An x indicates that an echo reply was received with an error code these packets are not counted in the received packets count. They are accounted for separately.

## Sample Output

### ping mpls l2vpn instance

```
user@host> ping mpls l2vpn instance vpn1 remote-site-id 1 local-site-id 2
!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

### ping mpls l2vpn instance detail

```
user@host> ping mpls l2vpn instance vpn1 remote-site-id 1 local-site-id 2 detail
Request for seq 1, to interface 68, labels <800001, 100176>
Reply for seq 1, return code: Egress-ok
Request for seq 2, to interface 68, labels <800001, 100176>
Reply for seq 2, return code: Egress-ok
Request for seq 3, to interface 68, labels <800001, 100176>
Reply for seq 3, return code: Egress-ok
Request for seq 4, to interface 68, labels <800001, 100176>
Reply for seq 4, return code: Egress-ok
Request for seq 5, to interface 68, labels <800001, 100176>
Reply for seq 5, return code: Egress-ok

--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

### ping mpls l2vpn interface <interface-name> reply-mode

```
user@host> ping mpls l2vpn interface lt-1/2/0.21 reply-mode ip-udp
!!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

## ping vpls instance

---

**Syntax** ping vpls instance *instance-name* destination-mac *address* source-ip *address*  
<bd-name *name*>  
<control-plane-response>  
<count *number*>  
<detail>  
<learning-vlan-id *number*>  
<logical-system *logical-system-name*>

**Release Information** Command introduced in Junos OS Release 9.1.

**Description** Check the operability of virtual private LAN service (VPLS) connections. Type Ctrl+c to interrupt a **ping vpls instance** command.

When you issue a **ping vpls instance** command, a chassis MAC address is drawn from the ingress PE router's pool of MAC addresses and used to create the VPLS ping packet. The ping packet is then forwarded to the egress PE router. When the egress PE router receives the ping packet, it learns the MAC address from the VPLS ping packet. The MAC address is added to the egress PE router's MAC table.

The **ping vpls instance** command relies on the LSP ping and trace infrastructure defined in RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures* and further enhancements defined in Internet draft draft-stokes-vkompella-ppvpn-hvpls-oam-02, *Testing Hierarchical Virtual Private LAN Services*.

**Options**

- instance *instance-name***—Specify the name of the VPLS routing instance.
- destination-mac *address***—Specify a destination MAC address for the ping echo requests.
- source ip *address***—IP address of the outgoing interface.
- bd-name *name***—(Optional) Name of the bridge domain.
- control-plane-response**—(Optional) Request VPLS OAM responses using the control plane.
- count *number***—(Optional) Number of ping requests to send. If **count** is not specified, five ping requests are sent. The range of values is 1 through 1,000,000. The default value is 5.
- detail**—(Optional) Display detailed information about the echo requests sent and received.
- learning-vlan-id *number***—(Optional) Specify a learning VLAN identifier for the ping echo requests. The range of values is 0 through 4094.
- logical-system *logical-system-name***—(Optional) Specify a logical system name for the ping echo requests.

**Additional Information** This statement is only supported on the MX Series routers, the M120 and M320 routers, and the T1600 router.

**Required Privilege Level** network

**List of Sample Output** [ping vpls instance on page 1251](#)

**Output Fields** When you enter this command, you are provided feedback on the status of your request. An exclamation point (!) indicates that an echo reply was received. A period (.) indicates that an echo reply was not received within the timeout period. An x indicates that an echo reply was received with an error code. Packets with an error code are not counted in the received packets count. They are accounted for separately.

## Sample Output

### [ping vpls instance](#)

```
user@host> ping vpls instance red destination-mac 00:89:67:1a:23:6f source-ip 10.255.17.138
! -> sample-router:red:ge-4/1/1.0
! -> sample-router:red:ge-4/1/1.0
! -> sample-router:red:ge-4/1/1.0
! -> sample-router:red:ge-4/1/1.0

--- vpls ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
```

## request l2circuit-switchover

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>request l2circuit-switchover</code><br><code>&lt;logical-system (all   logical-system-name)&gt;</code><br><code>&lt;neighbor address&gt;</code><br><code>&lt;virtual-circuit-id identifier&gt;</code>                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.2.<br>Statement introduced in Junos OS Release 14.1X53-D10 for the QFX Series and for EX4600 switches.                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | Manually trigger a switch from the active pseudowire to the redundant pseudowire. This command can be useful when performing network maintenance.                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <b>logical-system (all   <i>logical-system-name</i>)</b> —(Optional) Perform this operation on all logical systems or on a particular logical system.<br><br><b>neighbor address</b> —(Optional) Trigger a switch of all of the active pseudowire connections with the specified neighbor to their respective redundant pseudowires.<br><br><b>virtual-circuit-id <i>identifier</i></b> —(Optional) Trigger a switch from the active pseudowire connection of the specified Layer 2 circuit to its redundant pseudowire. |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>MPLS Feature Support on QFX Series and EX4600 Switches</i></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>List of Sample Output</b>    | <a href="#">request l2circuit-switchover virtual-circuit-id on page 1252</a>                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Sample Output

### request l2circuit-switchover virtual-circuit-id

```
user@host>request l2circuit-switchover virtual-circuit-id 12
```



## show evpn instance

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>show evpn instance &lt;brief   extensive&gt; &lt;backup-forwarder&gt; &lt;designated-forwarder&gt; &lt;esi esi&gt; &lt;instance-name&gt; &lt;neighbor neighbor-address&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | <p>Command introduced in Junos OS Release 14.1.</p> <p>Command introduced in Junos OS Release 14.2 for EX Series switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Show Ethernet VPN (EVPN) routing instance information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <p><b>none</b>—Display brief information about the EVPN routing instance.</p> <p><b>brief   extensive</b>—(Optional) Display the specified level of output.</p> <p><b>backup-forwarder</b>—(Optional) Display IP addresses of all the backup designated forwarder (non-DFs) for the Ethernet segment.</p> <p><b>designated-forwarder</b>—(Optional) Display IP address of the designated forwarder for the Ethernet segment.</p> <p><b>esi esi</b>—(Optional) Display brief information about the routing instance associated with this ESI value.</p> <p><b>instance-name</b>—(Optional) Display information for the specified routing instance.</p> <p><b>neighbor neighbor-address</b>—(Optional) Display IP address of the EVPN neighbor.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>List of Sample Output</b>    | <p><a href="#">show evpn instance brief on page 1255</a></p> <p><a href="#">show evpn instance on page 1255</a></p> <p><a href="#">show evpn instance extensive on page 1256</a></p> <p><a href="#">show evpn instance instance-name esi esi-value backup-forwarder on page 1257</a></p> <p><a href="#">show evpn instance instance-name esi esi-value designated-forwarder on page 1257</a></p>                                                                                                                                                                                                                                                                                                                                                  |
| <b>Output Fields</b>            | Table 24 on page 1253 lists the output fields for the <b>show evpn instance</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Table 24: show evpn instance Output Fields**

| Field Name      | Field Description                                                                                        | Level of Output |
|-----------------|----------------------------------------------------------------------------------------------------------|-----------------|
| <b>Instance</b> | Names of the routing instances.                                                                          | All Levels      |
| <b>Intfs</b>    | Total number of interfaces participating in each routing instance, and number of interfaces that are up. | <b>brief</b>    |

Table 24: show evpn instance Output Fields (*continued*)

| Field Name                         | Field Description                                                                                                                                                                                                                                                               | Level of Output  |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| IRB intfs                          | Statistics on number of IRB interfaces for each routing instance: <ul style="list-style-type: none"> <li><b>Total</b>—Total number of IRB interfaces.</li> <li><b>Up</b>—Number of active IRB interfaces.</li> <li><b>Nbrs</b>—Number of neighbor IRB interfaces.</li> </ul>    | <b>brief</b>     |
| MH ESIs                            | Number of Ethernet segments per routing instance that connect to a multihomed customer site.                                                                                                                                                                                    | <b>brief</b>     |
| MAC addresses                      | Number of local and remote MAC addresses for each routing instance.                                                                                                                                                                                                             | <b>brief</b>     |
| Route Distinguisher                | Unique route distinguisher associated with this routing instance.                                                                                                                                                                                                               | <b>extensive</b> |
| Per-instance MAC route label       | Label of MAC route for each routing instance.                                                                                                                                                                                                                                   | <b>extensive</b> |
| Per-instance multicast route label | Label of multicast route for each routing instance.                                                                                                                                                                                                                             | <b>extensive</b> |
| Total MAC addresses                | Total number of MAC addresses received for each routing instance.                                                                                                                                                                                                               | <b>extensive</b> |
| Default gateway MAC addresses      | Number of MAC addresses serving as a default gateway in the routing instance.                                                                                                                                                                                                   | <b>extensive</b> |
| Number of local interfaces         | Number of local interfaces belonging to this routing instance.                                                                                                                                                                                                                  | <b>extensive</b> |
| Interface name                     | Name of interfaces that belong to this routing instance.                                                                                                                                                                                                                        | <b>extensive</b> |
| ESI                                | Ethernet segment identifier (ESI) value of the interfaces belonging to this routing instance.                                                                                                                                                                                   | <b>extensive</b> |
| Mode                               | Mode of operation for each routing instance: <ul style="list-style-type: none"> <li><b>single-homed</b>—Default mode and does not require Ethernet segment values to be configured.</li> <li><b>single-active</b>—EVPN active-standby multihoming mode of operation.</li> </ul> | <b>extensive</b> |
| SH label                           | Split horizon label used for the active-standby multihoming mode of operation.                                                                                                                                                                                                  | <b>extensive</b> |
| Number of IRB interfaces           | Number of IRB interfaces that belong to this routing instance.                                                                                                                                                                                                                  | <b>extensive</b> |

Table 24: show evpn instance Output Fields (*continued*)

| Field Name                          | Field Description                                                                                                                                                                                                                                                                                                                                                                                                | Level of Output  |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <b>L3 context</b>                   | Names of routing instances that have the Layer 3 routes installed for an EVPN IRB interface, typically a VRF routing instance.                                                                                                                                                                                                                                                                                   | <b>extensive</b> |
| <b>Number of neighbors</b>          | Number of neighbors connected to this routing instance and their IP addresses.                                                                                                                                                                                                                                                                                                                                   | <b>extensive</b> |
| <b>MAC address advertisement</b>    | Number of MAC address advertisements received from the neighbor.                                                                                                                                                                                                                                                                                                                                                 | <b>extensive</b> |
| <b>MAC+IP address advertisement</b> | Number of MAC and IP address advertisements received from the neighbor.                                                                                                                                                                                                                                                                                                                                          | <b>extensive</b> |
| <b>Inclusive multicast</b>          | Number of inclusive multicast routes received from the neighbor.                                                                                                                                                                                                                                                                                                                                                 | <b>extensive</b> |
| <b>Ethernet auto-discovery</b>      | Number of autodiscovery routes per Ethernet segment received from the neighbor.                                                                                                                                                                                                                                                                                                                                  | <b>extensive</b> |
| <b>Number of ethernet segments</b>  | Total number of Ethernet segments for the routing instance.                                                                                                                                                                                                                                                                                                                                                      | <b>extensive</b> |
| <b>Designated forwarder</b>         | IP address of the designated forwarder (DF) for the Ethernet segment.                                                                                                                                                                                                                                                                                                                                            | <b>extensive</b> |
| <b>Backup forwarder</b>             | IP address of all the backup designated forwarders (BDFs) or non-DF routers for the Ethernet segment.<br><br><b>NOTE:</b> Immediately after an evpn interface esi value is changed and the new configuration is committed, the <b>Designated forwarder</b> information will change to <b>DF not elected yet</b> and the Backup forwarder information will not be displayed until after the election is complete. | <b>extensive</b> |

## Sample Output

### show evpn instance brief

```

user@host> show evpn instance brief

```

| Instance          | Intfs |    | IRB intfs |    | MH   |      | MAC addresses |        |  |
|-------------------|-------|----|-----------|----|------|------|---------------|--------|--|
|                   | Total | Up | Total     | Up | Nbrs | ESIs | Local         | Remote |  |
| ALPHA             | 2     | 2  | 1         | 1  | 2    | 1    | 3             | 4      |  |
| BETA              | 2     | 2  | 1         | 1  | 2    | 1    | 2             | 4      |  |
| __default__evpn__ | 0     | 0  | 0         | 0  | 1    | 0    | 0             | 0      |  |

### show evpn instance

```

user@host> show evpn instance
Instance: black
Route Distinguisher: 101:101
VLAN ID: 100
Label allocation mode: Per-instance

```

```

Per-instance MAC route label: 299776
Per-instance multicast route label: 299792
Number of local interfaces: 1
Number of local interfaces up: 1
 Interface name Static MACs ESI
 cbp-0.0 0 0
Number of neighbors: 1
 192.0.2.1
 Received routes
 MAC address advertisement: 1
 Ethernet auto-discovery: 0
 Inclusive multicast: 1

```

### show evpn instance extensive

```

user@host> show evpn instance extensive
Instance: ALPHA
 Route Distinguisher: 10.255.0.1:100
 Per-instance MAC route label: 300144
 Per-instance multicast route label: 300160
 MAC database status
 Local Remote
 Total MAC addresses: 3 4
 Default gateway MAC addresses: 1 2
 Number of local interfaces: 2 (2 up)
 Interface name ESI Mode SH label
 ae0.0 00:11:22:33:44:55:66:77:88:99 single-active
 ge-0/0/2.0 00:00:00:00:00:00:00:00:00:00 single-homed
 Number of IRB interfaces: 1 (1 up)
 Interface name L3 context
 irb.0 DELTA
 Number of neighbors: 2
 10.255.0.2
 Received routes
 MAC address advertisement: 2
 MAC+IP address advertisement: 3
 Inclusive multicast: 1
 Ethernet auto-discovery: 1
 10.255.0.3
 Received routes
 MAC address advertisement: 2
 MAC+IP address advertisement: 2
 Inclusive multicast: 1
 Ethernet auto-discovery: 0
 Number of ethernet segments: 1
 ESI: 00:11:22:33:44:55:66:77:88:99
 Designated forwarder: 10.255.0.1
 Backup forwarder: 10.255.0.2

Instance: BETA
 Route Distinguisher: 10.255.0.1:300
 VLAN ID: 300
 Per-instance MAC route label: 300176
 Per-instance multicast route label: 300192
 MAC database status
 Local Remote
 Total MAC addresses: 3 4
 Default gateway MAC addresses: 1 2
 Number of local interfaces: 2 (2 up)
 Interface name ESI Mode SH label
 ae1.0 00:00:00:00:00:00:00:00:00:00 single-homed
 ge-0/0/4.0 00:22:44:66:88:00:22:44:66:88 single-active
 Number of IRB interfaces: 1 (1 up)

```

```

Interface name L3 context
irb.1 DELTA
Number of neighbors: 2
10.255.0.2
 Received routes
 MAC address advertisement: 2
 MAC+IP address advertisement: 3
 Inclusive multicast: 1
 Ethernet auto-discovery: 1
10.255.0.3
 Received routes
 MAC address advertisement: 2
 MAC+IP address advertisement: 2
 Inclusive multicast: 1
 Ethernet auto-discovery: 0
Number of ethernet segments: 1
ESI: 00:22:44:66:88:00:22:44:66:88
Designated forwarder: 10.255.0.1
Backup forwarder: 10.255.0.2

Instance: __default_evpn__
Route Distinguisher: 10.255.0.1:0
VLAN ID: 0
Per-instance MAC route label: 300208
Per-instance multicast route label: 300224
MAC database status Local Remote
Total MAC addresses: 0 0
Default gateway MAC addresses: 0 0
Number of local interfaces: 0 (0 up)
Number of IRB interfaces: 0 (0 up)
Number of neighbors: 1
10.255.0.2
 Received routes
 Ethernet auto-discovery: 0
 Ethernet Segment: 2
Number of ethernet segments: 0

```

#### show evpn instance instance-name esi esi-value backup-forwarder

```

user@host> show evpn instance ALPHA esi 00:11:22:33:44:55:66:77:88:99 backup-forwarder
Instance: ALPHA
Number of ethernet segments: 1
ESI: 00:11:22:33:44:55:66:77:88:99
Backup forwarder: 10.255.0.2

```

#### show evpn instance instance-name esi esi-value designated-forwarder

```

user@host> show evpn instance ALPHA esi 00:11:22:33:44:55:66:77:88:99 designated-forwarder
Instance: ALPHA
Number of ethernet segments: 1
ESI: 00:11:22:33:44:55:66:77:88:99
Designated forwarder: 10.255.0.1

```

## show interfaces lsi (Label-Switched Interface)

**Syntax**    `show interfaces interface-type`  
               `<brief | detail | extensive | terse>`  
               `<descriptions>`  
               `<media>`  
               `<routing-instance instance-name>`  
               `<snmp-index snmp-index>`  
               `<statistics>`

**Release Information**    Command introduced before Junos OS Release 7.4.

**Description**    Display status information about the specified label-switched interface (LSI).

**Options**    *interface-type*—On most routers, the interface type is **lt-fpc/pic/port**.

**brief | detail | extensive | terse**—(Optional) Display the specified level of output.

**descriptions**—(Optional) Display interface description strings.

**media**—(Optional) Display media-specific information about network interfaces.

**routing-instance *instance-name***—(Optional) Display information for the specified routing instance.

**snmp-index *snmp-index***—(Optional) Display information for the specified SNMP index of the interface.

**statistics**—(Optional) Display static interface statistics.

**Required Privilege Level**    view

**Related Documentation**

**List of Sample Output**    [show interfaces lsi extensive on page 1260](#)

**Output Fields**    [Table 25 on page 1258](#) lists the output fields for the **show interfaces** (logical tunnel) command. Output fields are listed in the approximate order in which they appear.

**Table 25: Logical Tunnel show interfaces Output Fields**

| Field Name                | Field Description               | Level of Output |
|---------------------------|---------------------------------|-----------------|
| <b>Physical Interface</b> |                                 |                 |
| Physical interface        | Name of the physical interface. | All levels      |
| <b>Logical Interface</b>  |                                 |                 |
| Logical interface         | Name of the logical interface.  | All levels      |

Table 25: Logical Tunnel show interfaces Output Fields (*continued*)

| Field Name         | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Level of Output              |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Index              | Logical interface index number, which reflects its initialization sequence.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>detail extensive none</b> |
| SNMP ifIndex       | SNMP interface index number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <b>detail extensive none</b> |
| Generation         | Unique number for use by Juniper Networks technical support only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <b>detail extensive</b>      |
| Flags              | Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under <i>Common Output Fields Description</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | All levels                   |
| Encapsulation      | Encapsulation on the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | All levels                   |
| Traffic statistics | <p>Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</p> <ul style="list-style-type: none"> <li>• <b>Input bytes</b>—Rate of bytes received on the interface.</li> <li>• <b>Output bytes</b>—Rate of bytes transmitted on the interface.</li> <li>• <b>Input packets</b>—Rate of packets received on the interface.</li> <li>• <b>Output packets</b>—Rate of packets transmitted on the interface.</li> </ul> | <b>detail extensive</b>      |
| Local statistics   | Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>detail extensive</b>      |
| Transit statistics | Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>detail extensive</b>      |
| Protocol           | Protocol family configured on the logical interface, such as <b>iso</b> , <b>inet6</b> , <b>mpls</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <b>detail extensive none</b> |
| MTU                | MTU size on the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>detail extensive none</b> |
| Generation         | Unique number for use by Juniper Networks technical support only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <b>detail extensive</b>      |
| Flags              | Information about the protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <b>detail extensive none</b> |

## Sample Output

### show interfaces lsi extensive

```
user@host> show interfaces lsi extensive
```

```
Physical interface: lsi
```

```
Logical interface lsi.84934656 (Index 363) (SNMP ifIndex 586) (Generation 194)
```

```
Flags: Up Point-To-Point SNMP-Traps 0x4000000 Encapsulation: LSI-NULL
```

```
Traffic statistics:
```

```
Input bytes : 0
```

```
Output bytes : 0
```

```
Input packets: 0
```

```
Output packets: 0
```

```
Local statistics:
```

```
Input bytes : 0
```

```
Output bytes : 0
```

```
Input packets: 0
```

```
Output packets: 0
```

```
Transit statistics:
```

```
Input bytes : 0 0 bps
```

```
Output bytes : 0 0 bps
```

```
Input packets: 0 0 pps
```

```
Output packets: 0 0 pps
```

```
Protocol vpls, MTU: Unlimited, Generation: 279, Route table: 10
```

```
Logical interface lsi.84934657 (Index 366) (SNMP ifIndex 589) (Generation 197)
```

```
Flags: Up Point-To-Point SNMP-Traps 0x4000000 Encapsulation: LSI-NULL
```

```
Traffic statistics:
```

```
Input bytes : 0
```

```
Output bytes : 0
```

```
Input packets: 0
```

```
Output packets: 0
```

```
Local statistics:
```

```
Input bytes : 0
```

```
Output bytes : 0
```

```
Input packets: 0
```

```
Output packets: 0
```

```
Transit statistics:
```

```
Input bytes : 0 0 bps
```

```
Output bytes : 0 0 bps
```

```
Input packets: 0 0 pps
```

```
Output packets: 0 0 pps
```

```
Protocol vpls, MTU: Unlimited, Generation: 282, Route table: 10
```



## show l2circuit connections

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>show l2circuit connections &lt;brief   extensive   summary&gt; &lt;down   up   up-down&gt; &lt;history&gt; &lt;interface <i>interface-name</i>&gt; &lt;logical-system (all   <i>logical-system-name</i>)&gt; &lt;neighbor <i>neighbor</i>&gt; &lt;status&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | <p>Command introduced before Junos OS Release 7.4.</p> <p>Display enhancements in Junos OS Release 9.6.</p> <p>Display enhancements in Junos OS Release 10.2.</p> <p>Display enhancements in Junos OS Release 12.1.</p> <p>Display enhancements in Junos OS Release 13.2.</p> <p>Statement introduced in Junos OS Release 14.1X53-D10 for the QFX Series and for EX4600 switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Display status information about Layer 2 virtual circuits from the local provider edge (PE) router to its neighbors.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>                  | <p><b>none</b>—Display standard information about Layer 2 virtual circuits on all interfaces for all neighbors.</p> <p><b>brief   extensive   summary</b>—(Optional) Display the specified level of output. Use history to display information about connection history. Use status to display information about the connection and interface status.</p> <p><b>down   up   up-down</b>—(Optional) Display nonoperational, operational, or both kinds of connections.</p> <p><b>history</b>—(Optional) Display information about connection history.</p> <p><b>interface <i>interface-name</i></b>—(Optional) Show all Layer 2 virtual circuits on an interface.</p> <p><b>logical-system (all   <i>logical-system-name</i>)</b>—(Optional) Perform this operation on all logical systems or on a particular logical system.</p> <p><b>neighbor <i>neighbor</i></b>—(Optional) IP address of a specific neighbor.</p> <p><b>status</b>—(Optional) Display information about the connection and interface status.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>List of Sample Output</b>    | <p><a href="#">show l2circuit connections on page 1265</a></p> <p><a href="#">show l2circuit connections interface on page 1266</a></p> <p><a href="#">show l2circuit connections extensive on page 1266</a></p> <p><a href="#">show l2circuit connections extensive (Pseudowire Redundancy with Hot Standby) on page 1267</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**Output Fields** [Table 26 on page 1262](#) lists the output fields for the **show l2circuit connections** command. Output fields are listed in the approximate order in which they appear.

**Table 26: show l2circuit connections Output Fields**

| Field Name                         | Field Description                                                      |
|------------------------------------|------------------------------------------------------------------------|
| <b>Layer-2 Circuit Connections</b> | Displays the legends for connection and interface status.              |
| <b>Neighbor</b>                    | Remote PE neighbor.                                                    |
| <b>Interface</b>                   | Logical PE-to-CE interface on which the virtual circuit is configured. |
| <b>Type</b>                        | VC type: <b>rmt</b> (remote) or <b>loc</b> (local).                    |

Table 26: show l2circuit connections Output Fields (*continued*)

| Field Name                               | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Legend for connection status (St)</b> | <p>Status of the virtual circuit connection:</p> <ul style="list-style-type: none"> <li>• <b>EI</b>—The local virtual circuit interface is configured with an encapsulation that is not supported.</li> <li>• <b>MM</b>—The two routers do not agree on an MTU value, which causes an MTU mismatch.</li> <li>• <b>EM</b>—The encapsulation type received on this virtual circuit from the neighbor does not match the local virtual circuit interface encapsulation type.</li> <li>• <b>CM</b>—The two routers do not agree on a control word, which causes a control word mismatch.</li> <li>• <b>VM</b>—The remote and local VLAN IDs do not match across the Layer 2 circuit.</li> <li>• <b>OL</b>—No advertisement has been received for this virtual circuit from the neighbor. There is no outgoing label available for use by this virtual circuit.</li> <li>• <b>NC</b>—The interface is not configured as a CCC or TCC interface.</li> <li>• <b>BK</b>—The virtual circuit has switched to a backup connection.</li> <li>• <b>CB</b>—The remote PE router is advertising a different cell bundle from that configured on the local PE router.</li> <li>• <b>LD</b>—The connection to the local site is signaled down, because the CE-facing interface to the local site is down.</li> <li>• <b>RD</b>—The remote neighbor is down. It has signaled a problem using the pseudowire status code.</li> <li>• <b>NP</b>—The router detects that interface hardware is not present. The hardware may be offline, a PIC may not be of the desired type, or the interface may be configured in a different routing instance.</li> <li>• <b>Dn</b>—The virtual circuit is down.</li> <li>• <b>VC-Dn</b>—The virtual circuit is down because there is no tunnel LSP from the local PE router to the neighbor.</li> <li>• <b>UP</b>—The virtual circuit is operational.</li> <li>• <b>CF</b>—The router cannot find enough bandwidth to the remote router to satisfy the Layer 2 circuit bandwidth requirement.</li> <li>• <b>IB</b>—The bit rate is incompatible for Time Division Multiplexing (TDM).</li> <li>• <b>TDM</b>—TDM is not configured correctly.</li> <li>• <b>ST</b>—The virtual circuit has been switched to a standby connection.</li> <li>• <b>SP</b>—The virtual circuit connection is using a static pseudowire.</li> <li>• <b>RS</b>—The remote site is in a standby state.</li> <li>• <b>XX</b>—The virtual circuit is down for an unknown reason. This is a programming error.</li> </ul> |
| <b>Time last up</b>                      | Date and time the virtual circuit was last operational.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b># Up trans</b>                        | Number of times the virtual circuit came up.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>local-interface-name</b>              | Name of the local PE-to-CE interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Status</b>                            | Status of the local interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Up</b>                                | Interface is operational.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

Table 26: show l2circuit connections Output Fields (*continued*)

| Field Name                      | Field Description                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Dn</b>                       | Interface is not operational.                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>NP</b>                       | Not present. Interface does not exist.                                                                                                                                                                                                                                                                                                                                                                              |
| <b>DS</b>                       | Disabled. Interface has been administratively disabled.                                                                                                                                                                                                                                                                                                                                                             |
| <b>WE</b>                       | Wrong encapsulation. The interface is not configured as CCC.                                                                                                                                                                                                                                                                                                                                                        |
| <b>UN</b>                       | Interface status is initialized.                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Encapsulation</b>            | Encapsulation of the local interface.                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Remote PE</b>                | Prefix of the remote PE router.                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Negotiated control-word</b>  | Whether the use of the control word has been negotiated for this virtual circuit: <b>Yes (Null)</b> or <b>No</b> .                                                                                                                                                                                                                                                                                                  |
| <b>Incoming label</b>           | Label used by the remote side of the virtual circuit to send packets destined to the local side. This label is routed to the local virtual circuit interface.                                                                                                                                                                                                                                                       |
| <b>Outgoing label</b>           | Label used by the local side of the virtual circuit to send packets to the remote side of the virtual circuit. Packets originated on the local virtual circuit interface are encapsulated with this label before being placed on the tunnel LSP to the neighbor for this virtual circuit. This label is allocated by the neighbor and is used in demultiplexing incoming packets destined for this virtual circuit. |
| <b>Negotiated PW status TLV</b> | Displays the pseudowire status type, length, and value (TLV). TLVs are a method of encoding variable-length or optional information. If the pseudowire status TLV is used, the corresponding local or neighbor PE router status code is also displayed.                                                                                                                                                             |
| <b>local PW status code</b>     | If the pseudowire status TLV is used, displays the local PE router status code.                                                                                                                                                                                                                                                                                                                                     |
| <b>Neighbor PW status code</b>  | If the pseudowire status TLV is used, displays the neighbor PE router status code.                                                                                                                                                                                                                                                                                                                                  |
| <b>Local interface</b>          | Name of the local interface used for the Layer 2 circuit connection.                                                                                                                                                                                                                                                                                                                                                |
| <b>Status</b>                   | Status of the local interface ( <b>Up</b> or <b>Down</b> ).                                                                                                                                                                                                                                                                                                                                                         |
| <b>Encapsulation</b>            | Encapsulation configured for the local interface.                                                                                                                                                                                                                                                                                                                                                                   |
| <b>APS-active</b>               | Indicates that the interface belongs to the working circuit.                                                                                                                                                                                                                                                                                                                                                        |
| <b>APS-inactive</b>             | Indicates that the interface belongs to the protect circuit.                                                                                                                                                                                                                                                                                                                                                        |
| <b>Connection protection</b>    | Whether or not connection protection is configured for the Layer 2 circuit to the neighbor: <b>Yes</b> or <b>No</b> .                                                                                                                                                                                                                                                                                               |

Table 26: show l2circuit connections Output Fields (*continued*)

| Field Name         | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VC bandwidth       | Bandwidth requirement of the Layer 2 circuit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Time               | Time at which the event occurred.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Connection History | <p>Event types logged in history.</p> <ul style="list-style-type: none"> <li>• <b>loc intf up</b>—Local virtual circuit interface went up.</li> <li>• <b>loc intf down</b>—Local virtual circuit interface went down.</li> <li>• <b>In lbl Update</b>—Incoming label has been updated.</li> <li>• <b>Out lbl Update</b>—Outgoing label has been updated.</li> <li>• <b>PE route changed</b>—Route to PE router has been updated.</li> <li>• <b>PE route down</b>—Route to PE router is down.</li> <li>• <b>rmt side marked</b>—Remote side is marked.</li> <li>• <b>VC Dn</b>—Remote side indicated that its end of the virtual circuit is down (if the tunnel LSP from the remote side to the local side is down).</li> <li>• <b>status update timer</b>—Status update timer processing. It computes the state of the virtual circuit, and determines whether it should be advertised to or withdrawn from the remote side.</li> </ul> |

## Sample Output

### show l2circuit connections

```
user@host> show l2circuit connections
```

```
Layer-2 Circuit Connections:
```

```
Legend for connection status (St)
```

```

EI -- encapsulation invalid NP -- interface h/w not present
MM -- mtu mismatch Dn -- down
EM -- encapsulation mismatch VC-Dn -- Virtual circuit Down
CM -- control-word mismatch Up -- operational
VM -- vlan id mismatch CF -- Call admission control failure
OL -- no outgoing label IB -- TDM incompatible bitrate
NC -- intf encaps not CCC/TCC TM -- TDM misconfiguration
BK -- Backup Connection ST -- Standby Connection
CB -- rcvd cell-bundle size bad SP -- Static Pseudowire
LD -- local site signaled down RS -- remote site standby
RD -- remote site signaled down HS -- hot standby
XX -- unknown

```

```
Legend for interface status
```

```
Up -- operational
```

```
Dn -- down
```

```
Neighbor: 10.255.245.51
```

```

Interface Type St Time last up # Up trans
ge-2/0/2.600(vc 5) rmt Up Dec 7 18:11:18 2009 1
Remote PE: 10.255.245.51, Negotiated control-word: No
Incoming label: 299856, Outgoing label: 299808
Negotiated PW status TLV: No
Local interface: ge-2/0/2.600, Status: Up, Encapsulation: VLAN

```

## Sample Output

### show l2circuit connections interface

```

user@host> show l2circuit connections interface t1-2/0/0:1:1.0
Layer-2 Circuit Connections:

Legend for connection status (St)
EI -- encapsulation invalid NP -- interface h/w not present
MM -- mtu mismatch Dn -- down
EM -- encapsulation mismatch VC-Dn -- Virtual circuit Down
CM -- control-word mismatch Up -- operational
VM -- vlan id mismatch CF -- Call admission control failure
OL -- no outgoing label IB -- TDM incompatible bitrate
NC -- intf encaps not CCC/TCC TM -- TDM misconfiguration
BK -- Backup Connection ST -- Standby Connection
CB -- rcvd cell-bundle size bad SP -- Static Pseudowire
LD -- local site signaled down RS -- remote site standby
RD -- remote site signaled down HS -- hot standby
XX -- unknown

Legend for interface status
Up -- operational
Dn -- down
Neighbor: 10.1.1.1
 Interface Type St Time last up # Up trans
 t1-2/0/0:1:1.0(vc 1)(SP) rmt Up Apr 27 04:21:02 2011 1
 Remote PE: 10.1.1.1, Negotiated control-word: Yes (Non-null)
 Incoming label: 1010001, Outgoing label: 1000001
 Negotiated PW status TLV: No
 Local interface: t1-1/0/0:1:1.0, Status: Up, Encapsulation: SATOP-T1,
APS-active
 Local interface: t1-2/0/0:1:1.0, Status: Up, Encapsulation: SATOP-T1,
APS-inactive

```

## Sample Output

### show l2circuit connections extensive

```

user@host>show l2circuit connections extensive
Layer-2 Circuit Connections:

Legend for connection status (St)
EI -- encapsulation invalid NP -- interface h/w not present
MM -- mtu mismatch Dn -- down
EM -- encapsulation mismatch VC-Dn -- Virtual circuit Down
CM -- control-word mismatch Up -- operational
VM -- vlan id mismatch CF -- Call admission control failure
OL -- no outgoing label IB -- TDM incompatible bitrate
NC -- intf encaps not CCC/TCC TM -- TDM misconfiguration
BK -- Backup Connection ST -- Standby Connection
CB -- rcvd cell-bundle size bad SP -- Static Pseudowire
LD -- local site signaled down RS -- remote site standby
RD -- remote site signaled down HS -- hot standby
XX -- unknown

Legend for interface status
Up -- operational
Dn -- down
Neighbor: 10.255.49.149
 Interface Type St Time last up # Up trans

```

```

ae0.0(vc 100) rmt Up Aug 31 09:36:12 2009 1
Remote PE: 10.255.49.149, Negotiated control-word: Yes (Null)
Incoming label: 299824, Outgoing label: 299776
Negotiated PW status TLV: Yes
Local PW status code: 0x00000000, Neighbor PW status code: 0x00000000
Local interface: ae0.0, Status: Up, Encapsulation: ETHERNET
Connection protection: Yes
Connection History:
 Aug 31 09:36:12 2009 status update timer
 Aug 31 09:36:12 2009 PE route changed
 Aug 31 09:36:12 2009 Out lbl Update 299776
 Aug 31 09:36:12 2009 In lbl Update 299824
 Aug 31 09:36:12 2009 loc intf up ae0.0

```

## Sample Output

### show l2circuit connections extensive (Pseudowire Redundancy with Hot Standby)

```
user@host>show l2circuit connections extensive
```

Layer-2 Circuit Connections:

Legend for connection status (St)

|                                 |                                      |
|---------------------------------|--------------------------------------|
| EI -- encapsulation invalid     | NP -- interface h/w not present      |
| MM -- mtu mismatch              | Dn -- down                           |
| EM -- encapsulation mismatch    | VC-Dn -- Virtual circuit Down        |
| CM -- control-word mismatch     | Up -- operational                    |
| VM -- vlan id mismatch          | CF -- Call admission control failure |
| OL -- no outgoing label         | IB -- TDM incompatible bitrate       |
| NC -- intf encaps not CCC/TCC   | TM -- TDM misconfiguration           |
| BK -- Backup Connection         | ST -- Standby Connection             |
| CB -- rcvd cell-bundle size bad | SP -- Static Pseudowire              |
| LD -- local site signaled down  | RS -- remote site standby            |
| RD -- remote site signaled down | HS -- Hot-standby Connection         |
| XX -- unknown                   |                                      |

Legend for interface status

Up -- operational

Dn -- down

Neighbor: 192.0.2.101

```

Interface Type St Time last up # Up trans
ge-1/3/2.600(vc 1) rmt Up Jan 24 11:00:26 2013 1
Remote PE: 192.0.2.101, Negotiated control-word: Yes (Null)
Incoming label: 299776, Outgoing label: 299776
Negotiated PW status TLV: Yes
Local PW status code: 0x00000000, Neighbor PW status code: 0x00000000
Local interface: ge-1/3/2.600, Status: Up, Encapsulation: VLAN
Connection History:
 Jan 24 11:00:26 2013 status update timer
 Jan 24 11:00:26 2013 PE route changed
 Jan 24 11:00:26 2013 Out lbl Update 299776
 Jan 24 11:00:26 2013 In lbl Update 299776
 Jan 24 11:00:26 2013 loc intf up ge-1/3/2.600

```

Neighbor: 192.0.2.102

```

Interface Type St Time last up # Up trans
ge-1/3/2.600(vc 2) rmt HS ----- ----
Remote PE: 192.0.2.102, Negotiated control-word: Yes (Null)
Incoming label: 299792, Outgoing label: 299776
Negotiated PW status TLV: Yes
Local PW status code: 0x00000020, Neighbor PW status code: 0x00000000
Local interface: ge-1/3/2.600, Status: Up, Encapsulation: VLAN

```





## show l2vpn connections

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>show l2vpn connections &lt;brief   extensive&gt; &lt;down   up   up-down&gt; &lt;history&gt; &lt;instance <i>instance</i>&gt; &lt;instance-history&gt; &lt;local-site <i>local-site</i>&gt; &lt;logical-system (all   <i>logical-system-name</i>)&gt; &lt;remote-site <i>remote-site</i>&gt; &lt;status&gt; &lt;summary&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | <p>Command introduced before Junos OS Release 7.4.</p> <p><b>instance-history</b> option introduced in Junos OS Release 12.3R2.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | Display Layer 2 virtual private network (VPN) connections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <p><b>none</b>—Display all Layer 2 VPN connections for all routing instances.</p> <p><b>brief   extensive</b>—(Optional) Display the specified level of output.</p> <p><b>down   up   up-down</b>—(Optional) Display nonoperational, operational, or both kinds of connections.</p> <p><b>history</b>—(Optional) Display information about connection history.</p> <p><b>instance <i>instance</i></b>—(Optional) Display connections for the specified routing instance only.</p> <p><b>instance-history</b>—(Optional) Display information about connection history for a particular instance.</p> <p><b>local-site <i>local-site</i></b>—(Optional) Display connections for the specified Layer 2 VPN local site name or ID only.</p> <p><b>logical-system (all   <i>logical-system-name</i>)</b>—(Optional) Perform this operation on all logical systems or on a particular logical system.</p> <p><b>remote-site <i>remote-site</i></b>—(Optional) Display connection for the specified Layer 2 VPN remote site ID only.</p> <p><b>status</b>—(Optional) Display information about the connection and interface status.</p> <p><b>summary</b>—(Optional) Display summary of all Layer 2 VPN connections information.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>List of Sample Output</b>    | <p><a href="#">show l2vpn connections on page 1272</a></p> <p><a href="#">show l2vpn connections extensive on page 1273</a></p> <p><a href="#">show l2vpn connections extensive (VPWS) on page 1273</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**Output Fields** Table 27 on page 1270 lists the output fields for the **show l2vpn connections** command. Output fields are listed in the approximate order in which they appear.

**Table 27: show l2vpn connections Output Fields**

| Field Name                        | Field Description                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Instance</b>                   | Name of Layer 2 VPN instance.                                                                                                                                                                                                                                                                                                                                                                  |
| <b>L2vpn-id</b>                   | For BGP autodiscovery, a globally unique Layer 2 VPN community identifier for the instance.                                                                                                                                                                                                                                                                                                    |
| <b>Local-ID</b>                   | BGP <b>local-address</b> assigned to the local routing device.                                                                                                                                                                                                                                                                                                                                 |
| <b>Local site</b>                 | Name of local site.                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Local source-attachment-id</b> | For FEC 129, the VPWS source attachment identifier. The point-to-point nature of VPWS requires that you specify the source access individual identifier (SAII) and the target access individual identifier (TAII). This SAII-TAII pair defines a unique pseudowire between two PE devices.                                                                                                     |
| <b>Target-attachment-id</b>       | For FEC 129, the VPWS target attachment identifier. If the configured target identifier matches a source identifier advertised by a remote PE device by way of a BGP auto-discovery message, the pseudowire between that source-target pair is signaled. If there is no match between an advertised source identifier and the configured target identifier, the pseudowire is not established. |
| <b>Interface name</b>             | Name of interface.                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Remote Site ID</b>             | Remote site ID.                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Label Offset</b>               | Numbers within the label block that are skipped to find the next label base.                                                                                                                                                                                                                                                                                                                   |
| <b>Label-base</b>                 | Advertises the first label in a block of labels. A remote PE router uses this first label when sending traffic toward the advertising PE router.                                                                                                                                                                                                                                               |
| <b>Range</b>                      | Advertises the label block size.                                                                                                                                                                                                                                                                                                                                                               |
| <b>status-vector</b>              | Bit vector advertising the state of local PE-CE circuits to remote PE routers. A bit value of <b>0</b> indicates that the local circuit and LSP tunnel to the remote PE router are up, whereas a value of <b>1</b> indicates either one or both are down.                                                                                                                                      |
| <b>connection-site</b>            | Name of the connection site.                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Type</b>                       | Type of connection: <b>loc</b> (local) or <b>rmt</b> (remote).                                                                                                                                                                                                                                                                                                                                 |
| <b>St</b>                         | Status of the connection. (For a list of possible values, see the <b>Legend for connection status (St)</b> field.)                                                                                                                                                                                                                                                                             |
| <b>Time last up</b>               | Time that the connection was last in the <b>Up</b> condition.                                                                                                                                                                                                                                                                                                                                  |
| <b># Up trans</b>                 | Number of transitions from <b>Down</b> to <b>Up</b> condition.                                                                                                                                                                                                                                                                                                                                 |

Table 27: show l2vpn connections Output Fields (*continued*)

| Field Name            | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Local circuit</b>  | Address and status of local circuit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Remote circuit</b> | Address and status of remote circuit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>St</b>             | <p>Status of the Layer 2 VPN connection (corresponds with Legend for Connection Status):</p> <ul style="list-style-type: none"> <li>• <b>EI</b>—The local Layer 2 VPN interface is configured with an encapsulation that is not supported.</li> <li>• <b>EM</b>—The encapsulation type received on this Layer 2 VPN connection from the neighbor does not match the local Layer 2 VPN connection interface encapsulation type.</li> <li>• <b>VC-Dn</b>—The virtual circuit is currently down.</li> <li>• <b>CM</b>—The two routers do not agree on a control word, which causes a control word mismatch.</li> <li>• <b>CN</b>—The virtual circuit is not provisioned properly.</li> <li>• <b>OR</b>—The label associated with the virtual circuit is out of range.</li> <li>• <b>OL</b>—No advertisement has been received for this virtual circuit from the neighbor. There is no outgoing label available for use by this virtual circuit.</li> <li>• <b>LD</b>—All of the CE-facing interfaces to the local site are down. Therefore, the connection to the local site is signaled as down to the other PE routers. No pseudowires can be established.</li> <li>• <b>RD</b>—All the interfaces to the remote neighbor are down. Therefore, the remote site has been signaled as down to the other PE routers. No pseudowires can be established.</li> <li>• <b>LN</b>—The local site has lost path selection to the remote site and therefore no pseudowires can be established from this local site.</li> <li>• <b>RN</b>—The remote site has lost path selection to a local site or other remote site and therefore no pseudowires are established to this remote site.</li> <li>• <b>XX</b>—The Layer 2 VPN connection is down for an unknown reason. This is a programming error.</li> <li>• <b>NC</b>—The interface encapsulation is not configured as an appropriate CCC, TCC, or Layer 2 VPN encapsulation.</li> <li>• <b>WE</b>—The encapsulation configured for the interface does not match the encapsulation configured for the associated connection within the Layer 2 VPN routing instance.</li> <li>• <b>NP</b>—The router detects that interface hardware is not present. The hardware might be offline, a PIC might not be of the desired type, or the interface might be configured in a different routing instance.</li> <li>• <b>-&gt;</b>—Only the outbound connection is up.</li> <li>• <b>&lt;-</b>—Only the inbound connection is up.</li> <li>• <b>Up</b>—The Layer 2 VPN connection is operational.</li> <li>• <b>Dn</b>—The Layer 2 VPN connection is down.</li> <li>• <b>CF</b>—The router cannot find enough bandwidth to the remote router to satisfy the Layer 2 VPN connection bandwidth requirement.</li> <li>• <b>SC</b>—The local site identifier matches the remote site identifier. No pseudowire can be established between these two sites. You should configure different values for the local and remote site identifiers.</li> </ul> |

Table 27: show l2vpn connections Output Fields (*continued*)

| Field Name        | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | <ul style="list-style-type: none"> <li><b>LM</b>—The local site identifier is not the minimum designated, meaning it is not the lowest. There is another local site with a lower site identifier. Pseudowires are not being established to this local site, and the associated local site identifier is not being used to distribute Layer 2 VPN label blocks. However, this is not an error state. Traffic continues to be forwarded to the PE router interfaces connected to the local sites when the local sites are in this state.</li> <li><b>RM</b>—The remote site identifier is not the minimum designated, meaning it is not the lowest. There is another remote site connected to the same PE router which has lower site identifier. The PE router cannot establish a pseudowire to this remote site and the associated remote site identifier cannot be used to distribute VPLS label blocks. However, this is not an error state. Traffic can continue to be forwarded to the PE router interface connected to this remote site when the remote site is in this state.</li> <li><b>IL</b>—The incoming packets for the Layer 2 VPN connection have no MPLS label.</li> </ul> |
| Remote PE         | Address of the remote provider edge router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Incoming label    | Name of the incoming label.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Outgoing label    | Name of the outgoing label.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Egress Protection | Whether the given PVC is protected by connection protection logic using egress protection for BGP signaled layer 2 services.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Time              | Date and time of Layer 2 VPN connection event.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Event             | Type of event.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Interface/Lbl/PE  | Interface, label, or PE router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Sample Output

### show l2vpn connections

```

user@host> show l2vpn connections
L2VPN Connections :
Instance : vpna
Edge protection: Not-Primary
Local site: 2 (ce-2)
offset: 1, range: 3, label-base: 32768
 connection-site Type St Time last up # Up trans
 3 (3) loc Up Jul 18 20:45:46 2001 1
 Local circuit: fe-0/0/0.1, Status: Up
 Remote circuit: fe-0/0/3.0, Status: Up
 1 rmt Up Jul 18 21:47:25 2001 1
 Local circuit: fe-0/0/0.0, Status: Up
 Remote PE: 192.0.2.1
 Incoming label: 32768, Outgoing label: 32769
Local site: 3 (ce-3)
offset: 1, range: 2, label-base: 33792
 connection-site Type St Time last up # Up trans

```

```

2 (ce-b) loc Up Jul 18 20:45:46 2001 1
 Local circuit: fe-0/0/0.1, Status: Up
 Remote circuit: fe-0/0/3.0, Status: Up
1 rmt Up Jul 18 21:47:25 2001 1
 Local circuit: fe-0/0/3.1, Status: Up
 Remote PE: 192.0.2.1
 Incoming label: 33792, Outgoing label: 32770

```

### show l2vpn connections extensive

```

user@host> show l2vpn connections extensive
L2VPN Connections:
Instance: vpn-a
Edge protection: Not-Primary
Local site: ce-a (1)
 Interface name Remote Site ID
 fe-0/0/0.0 2
 Label Offset Offset Range
 32768 1 2
 connection-site Type St Time last up # Up trans
 2 rmt Up Aug 3 00:08:14 2001 1
 Local circuit: fe-0/0/0.0, Status: Up
 Remote PE: 192.168.24.1
 Incoming label: 32769, Outgoing label: 32768
 Egress Protection: Yes
 Time Event Interface/Lbl/PE
 Aug 3 00:08:14 2001 PE route up
 Aug 3 00:08:14 2001 Out lbl Update 32768
 Aug 3 00:08:14 2001 In lbl Update 32769
 Aug 3 00:08:14 2001 ckt0 up fe-0/0/0.0

```

### show l2vpn connections extensive (VPWS)

```

user@host> show l2vpn connections
Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down NP -- interface hardware not present
CM -- control-word mismatch -> -- only outbound connection is up
CN -- circuit not provisioned <- -- only inbound connection is up
OR -- out of range Up -- operational
OL -- no outgoing label Dn -- down
LD -- local site signaled down CF -- call admission control failure
RD -- remote site signaled down SC -- local and remote site ID collision
LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status IL -- no incoming label
MM -- MTU mismatch MI -- Mesh-Group ID not available
BK -- Backup connection ST -- Standby connection
PF -- Profile parse failure PB -- Profile busy
RS -- remote site standby SN -- Static Neighbor
LB -- Local site not best-site RB -- Remote site not best-site
VM -- VLAN ID mismatch

Legend for interface status
Up -- operational
Dn -- down

Instance: FEC129-VPWS

```

```
L2vpn-id: 100:100
Number of local interfaces: 1
Number of local interfaces up: 1
ge-2/0/5.0
Local source-attachment-id: 1 (ONE)
Target-attachment-id Type St Time last up # Up trans
2 rmt Up Nov 28 16:16:14 2012 1
 Remote PE: 198.51.100.2, Negotiated control-word: No
 Incoming label: 299792, Outgoing label: 299792
 Local interface: ge-2/0/5.0, Status: Up, Encapsulation: ETHERNET
Connection History:
 Nov 28 16:16:14 2012 status update timer
 Nov 28 16:16:14 2012 PE route changed
 Nov 28 16:16:14 2012 Out lbl Update 299792
 Nov 28 16:16:14 2012 In lbl Update 299792
 Nov 28 16:16:14 2012 loc intf up ge-2/0/5.0
```

## show pim snooping interfaces

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show pim snooping interfaces<br><brief   detail><br><instance <i>instance-name</i> ><br><interface <i>interface-name</i> ><br><logical-system <i>logical-system-name</i> ><br><vlan-id <i>vlan-identifier</i> >                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Command introduced in Junos OS Release 12.3 for MX Series 3D Universal Edge devices.<br>Command introduced in Junos OS Release 13.2 for M Series Multiservice Edge devices.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Display information about PIM snooping interfaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>                  | <p><b>none</b>—Display detailed information.</p> <p><b>brief   detail</b>—(Optional) Display the specified level of output.</p> <p><b>instance &lt;instance-name&gt;</b>—(Optional) Display PIM snooping interface information for the specified routing instance.</p> <p><b>interface &lt;interface-name&gt;</b>—(Optional) Display PIM snooping information for the specified interface only.</p> <p><b>logical-system <i>logical-system-name</i></b>—(Optional) Display information about a particular logical system, or type 'all'.</p> <p><b>vlan-id &lt;vlan-identifier&gt;</b>—(Optional) Display PIM snooping interface information for the specified VLAN.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>PIM Snooping for VPLS</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>List of Sample Output</b>    | <a href="#">show pim snooping interfaces on page 1276</a><br><a href="#">show pim snooping interfaces instance vpls1 on page 1276</a><br><a href="#">show pim snooping interfaces interface &lt;interface-name&gt; on page 1277</a><br><a href="#">show pim snooping interfaces vlan-id &lt;vlan-id&gt; on page 1277</a>                                                                                                                                                                                                                                                                                                                                                 |
| <b>Output Fields</b>            | Table 28 on page 1275 lists the output fields for the <b>show pim snooping interface</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

Table 28: show pim snooping interface Output Fields

| Field Name      | Field Description                  | Level of Output |
|-----------------|------------------------------------|-----------------|
| Instance        | Routing instance for PIM snooping. | All levels      |
| Learning-Domain | Learning domain for snooping.      | All levels      |

Table 28: show pim snooping interface Output Fields (*continued*)

| Field Name        | Field Description                                                        | Level of Output |
|-------------------|--------------------------------------------------------------------------|-----------------|
| <b>Name</b>       | Router interfaces that are part of this learning domain.                 | All levels      |
| <b>State</b>      | State of the interface: <b>Up</b> , or <b>Down</b> .                     | All levels      |
| <b>IP-Version</b> | Version of IP used: 4 for IPv4, or 6 for IPv6.                           | All levels      |
| <b>NbrCnt</b>     | Number of neighboring routers connected through the specified interface. | All levels      |
| <b>DR address</b> | IP address of the designated router.                                     | All levels      |

## Sample Output

### show pim snooping interfaces

```

user@host> show pim snooping interfaces
Instance: vpls1
Learning-Domain: vlan-id 10
Name State IP-Version NbrCnt
ge-1/3/1.10 Up 4 1
ge-1/3/3.10 Up 4 1
ge-1/3/5.10 Up 4 1
ge-1/3/7.10 Up 4 1
DR address: 192.0.2.5
DR flooding is ON

Learning-Domain: vlan-id 20
Name State IP-Version NbrCnt
ge-1/3/1.20 Up 4 1
ge-1/3/3.20 Up 4 1
ge-1/3/5.20 Up 4 1
ge-1/3/7.20 Up 4 1
DR address: 192.0.2.6
DR flooding is ON

```

### show pim snooping interfaces instance vpls1

```

user@host> show pim snooping interfaces instance vpls1
Instance: vpls1

Learning-Domain: vlan-id 10
Name State IP-Version NbrCnt
ge-1/3/1.10 Up 4 1
ge-1/3/3.10 Up 4 1
ge-1/3/5.10 Up 4 1
ge-1/3/7.10 Up 4 1
DR address: 192.0.2.5
DR flooding is ON

Learning-Domain: vlan-id 20
Name State IP-Version NbrCnt
ge-1/3/1.20 Up 4 1
ge-1/3/3.20 Up 4 1
ge-1/3/5.20 Up 4 1
ge-1/3/7.20 Up 4 1

```



```
DR address: 192.0.2.6
DR flooding is ON
```

#### show pim snooping interfaces interface <interface-name>

```
user@host> show pim snooping interfaces interface ge-1/3/1.10
Instance: vpls1
Learning-Domain: vlan-id 10

Name State IP-Version NbrCnt
ge-1/3/1.10 Up 4 1
DR address: 192.0.2.5
DR flooding is ON

Learning-Domain: vlan-id 20
DR address: 192.0.2.6
DR flooding is ON
```

#### show pim snooping interfaces vlan-id <vlan-id>

```
user@host> show pim snooping interfaces vlan-id 10
Instance: vpls1
Learning-Domain: vlan-id 10

Name State IP-Version NbrCnt
ge-1/3/1.10 Up 4 1
ge-1/3/3.10 Up 4 1
ge-1/3/5.10 Up 4 1
ge-1/3/7.10 Up 4 1
DR address: 192.0.2.5
DR flooding is ON
```

## show pim snooping join

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show pim snooping join<br><brief   detail   extensive><br><instance <i>instance-name</i> ><br><logical-system <i>logical-system-name</i> ><br><vlan-id <i>vlan-id</i> >                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Command introduced in Junos OS Release 12.3 for MX Series 3D Universal Edge devices.<br>Command introduced in Junos OS Release 13.2 for M Series Multiservice Edge devices.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | Display information about Protocol Independent Multicast (PIM) snooping joins.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <p><b>none</b>—Display detailed information.</p> <p><b>brief   detail   extensive</b>—(Optional) Display the specified level of output.</p> <p><b>instance <i>instance-name</i></b>—(Optional) Display PIM snooping join information for the specified routing instance.</p> <p><b>logical-system <i>logical-system-name</i></b>—(Optional) Display information about a particular logical system, or type 'all'.</p> <p><b>vlan-id <i>vlan-identifier</i></b>—(Optional) Display PIM snooping join information for the specified VLAN.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><i>PIM Snooping for VPLS</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>List of Sample Output</b>    | <a href="#">show pim snooping join on page 1280</a><br><a href="#">show pim snooping join extensive on page 1280</a><br><a href="#">show pim snooping join instance on page 1280</a><br><a href="#">show pim snooping join vlan-id on page 1281</a>                                                                                                                                                                                                                                                                                         |
| <b>Output Fields</b>            | Table 29 on page 1278 lists the output fields for the <b>show pim snooping join</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                        |

**Table 29: show pim snooping join Output Fields**

| Field Name      | Field Description                  | Level of Output |
|-----------------|------------------------------------|-----------------|
| Instance        | Routing instance for PIM snooping. | All levels      |
| Learning-Domain | Learning domain for PIM snooping.  | All levels      |
| Group           | Multicast group address.           | All levels      |

Table 29: show pim snooping join Output Fields (*continued*)

| Field Name           | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Level of Output  |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Source               | Multicast source address: <ul style="list-style-type: none"> <li>• * (wildcard value)</li> <li>• &lt;ipv4-address&gt;</li> <li>• &lt;ipv6-address&gt;</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | All levels       |
| Flags                | PIM flags: <ul style="list-style-type: none"> <li>• <b>bidirectional</b>—Bidirectional mode entry.</li> <li>• <b>dense</b>—Dense mode entry.</li> <li>• <b>rptree</b>—Entry is on the rendezvous point tree.</li> <li>• <b>sparse</b>—Sparse mode entry.</li> <li>• <b>spt</b>—Entry is on the shortest-path tree for the source.</li> <li>• <b>wildcard</b>—Entry is on the shared tree.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                     | All levels       |
| Upstream state       | Information about the upstream interface: <ul style="list-style-type: none"> <li>• <b>Join to RP</b>—Sending a join to the rendezvous point.</li> <li>• <b>Join to Source</b>—Sending a join to the source.</li> <li>• <b>Local RP</b>—Sending neither join messages nor prune messages toward the RP, because this router is the rendezvous point.</li> <li>• <b>Local Source</b>—Sending neither join messages nor prune messages toward the source, because the source is locally attached to this routing device.</li> <li>• <b>Prune to RP</b>—Sending a prune to the rendezvous point.</li> <li>• <b>Prune to Source</b>—Sending a prune to the source.</li> </ul> <p><b>NOTE:</b> RP group range entries have <b>None</b> in the <b>Upstream state</b> field because RP group ranges do not trigger actual PIM join messages between routers.</p> | All levels       |
| Upstream neighbor    | Information about the upstream neighbor: <b>Direct</b> , <b>Local</b> , <b>Unknown</b> , or a specific IP address. <p>For bidirectional PIM, <b>Direct</b> means that the interface is directly connected to a subnet that contains a phantom RP address.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | All levels       |
| Upstream port        | RPF interface toward the source address for the source-specific state (S,G) or toward the rendezvous point (RP) address for the non-source-specific state (*G). <p>For bidirectional PIM, <b>RP Link</b> means that the interface is directly connected to a subnet that contains a phantom RP address.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | All levels       |
| Downstream port      | Information about downstream interfaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>extensive</b> |
| Downstream neighbors | Address of the downstream neighbor.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>extensive</b> |
| Timeout              | Time remaining until the downstream join state is updated (in seconds).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <b>extensive</b> |

## Sample Output

### show pim snooping join

```
user@host> show pim snooping join
Instance: vpls1

Learning-Domain: vlan-id 10
Group: 198.51.100.2
Source: *
Flags: sparse,rptree,wildcard
Upstream state: None
Upstream neighbor: 192.0.2.4, port: ge-1/3/5.10

Learning-Domain: vlan-id 20
Group: 198.51.100.3
Source: *
Flags: sparse,rptree,wildcard
Upstream state: None
Upstream neighbor: 203.0.113.4, port: ge-1/3/5.20
```

### show pim snooping join extensive

```
user@host> show pim snooping join extensive
Instance: vpls1
Learning-Domain: vlan-id 10

Group: 198.51.100.2
Source: *
Flags: sparse,rptree,wildcard
Upstream state: None
Upstream neighbor: 192.0.2.4, port: ge-1/3/5.10
Downstream port: ge-1/3/1.10
Downstream neighbors:
192.0.2.2 State: Join Flags: SRW Timeout: 166

Learning-Domain: vlan-id 20
Group: 198.51.100.3
Source: *
Flags: sparse,rptree,wildcard
Upstream state: None
Upstream neighbor: 203.0.113.4, port: ge-1/3/5.20
Downstream port: ge-1/3/3.20
Downstream neighbors:
203.0.113.3 State: Join Flags: SRW Timeout: 168
```

### show pim snooping join instance

```
user@host> show pim snooping join instance vpls1
Instance: vpls1

Learning-Domain: vlan-id 10
Group: 198.51.100.2
Source: *
Flags: sparse,rptree,wildcard
Upstream state: None
Upstream neighbor: 192.0.2.4, port: ge-1/3/5.10

Learning-Domain: vlan-id 20
Group: 198.51.100.3
```

Source: \*  
Flags: sparse,rptree,wildcard  
Upstream state: None  
Upstream neighbor: 203.0.113.4, port: ge-1/3/5.20

#### show pim snooping join vlan-id

```
user@host> show pim snooping join vlan-id 10
Instance: vpls1
Learning-Domain: vlan-id 10
Group: 198.51.100.2
Source: *
Flags: sparse,rptree,wildcard
Upstream state: None
Upstream neighbor: 192.0.2.4, port: ge-1/3/5.10
```

## show pim snooping neighbors

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show pim snooping neighbors</code><br><code>&lt;brief   detail&gt;</code><br><code>&lt;instance <i>instance-name</i>&gt;</code><br><code>&lt;interface <i>interface-name</i>&gt;</code><br><code>&lt;logical-system <i>logical-system-name</i>&gt;</code><br><code>&lt;vlan-id <i>vlan-identifier</i>&gt;</code>                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Command introduced in Junos OS Release 12.3 for MX Series 3D Universal Edge devices.<br>Command introduced in Junos OS Release 13.2 for M Series Multiservice Edge devices.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | Display information about Protocol Independent Multicast (PIM) snooping neighbors.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Options</b>                  | <b>none</b> —Display detailed information.<br><br><b>brief   detail</b> —(Optional) Display the specified level of output.<br><br><b>instance <i>instance-name</i></b> —(Optional) Display PIM snooping neighbor information for the specified routing instance.<br><br><b>interface <i>interface-name</i></b> —(Optional) Display information for the specified PIM snooping neighbor interface.<br><br><b>logical-system <i>logical-system-name</i></b> —(Optional) Display information about a particular logical system, or type 'all'.<br><br><b>vlan-id <i>vlan-identifier</i></b> —(Optional) Display PIM snooping neighbor information for the specified VLAN. |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Configuring Interface Priority for PIM Designated Router Selection</i></li><li>• <i>Modifying the PIM Hello Interval</i></li><li>• <i>PIM Snooping for VPLS</i></li><li>• <i>show pim neighbors</i></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>List of Sample Output</b>    | <a href="#">show pim snooping neighbors on page 1283</a><br><a href="#">show pim snooping neighbors detail on page 1284</a><br><a href="#">show pim snooping neighbors instance on page 1285</a><br><a href="#">show pim snooping neighbors interface on page 1285</a><br><a href="#">show pim snooping neighbors vlan-id on page 1286</a>                                                                                                                                                                                                                                                                                                                             |
| <b>Output Fields</b>            | <a href="#">Table 30 on page 1283</a> lists the output fields for the <b>show pim snooping neighbors</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Table 30: show pim snooping neighbors Output Fields

| Field Name                          | Field Description                                                                                                                                                                                                                                                                             | Level of Output |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Instance</b>                     | Routing instance for PIM snooping.                                                                                                                                                                                                                                                            | All levels      |
| <b>Learning-Domain</b>              | Learning domain for PIM snooping.                                                                                                                                                                                                                                                             | All levels      |
| <b>Interface</b>                    | Router interface for which PIM snooping neighbor details are displayed.                                                                                                                                                                                                                       | All levels      |
| <b>Option</b>                       | PIM snooping options available on the specified interface: <ul style="list-style-type: none"> <li>• H = Hello Option Holdtime</li> <li>• P = Hello Option DR Priority</li> <li>• L = Hello Option LAN Prune Delay</li> <li>• G = Generation Identifier</li> <li>• T = Tracking Bit</li> </ul> | All levels      |
| <b>Uptime</b>                       | Time the neighbor has been operational since the PIM process was last initialized, in the format <b>dd:hh:mm:ss ago</b> for less than a week and <b>nwnd:hh:mm:ss ago</b> for more than a week.                                                                                               | All levels      |
| <b>Neighbor addr</b>                | IP address of the PIM snooping neighbor connected through the specified interface.                                                                                                                                                                                                            | All levels      |
| <b>Address</b>                      | IP address of the specified router interface.                                                                                                                                                                                                                                                 | All levels      |
| <b>Hello Option Holdtime</b>        | Time for which the neighbor is available, in seconds. The range of values is <b>0</b> through <b>65,535</b> .                                                                                                                                                                                 | <b>detail</b>   |
| <b>Hello Option DR Priority</b>     | Designated router election priority. The range of values is <b>0</b> through <b>4294967295</b> .<br><br><b>NOTE:</b> By default, every PIM interface has an equal probability (priority 1) of being selected as the DR.                                                                       | <b>detail</b>   |
| <b>Hello Option Generation ID</b>   | 9-digit or 10-digit number used to tag hello messages.                                                                                                                                                                                                                                        | <b>detail</b>   |
| <b>Hello Option LAN Prune Delay</b> | Time to wait before the neighbor receives prune messages, in the format <b>delay nnn ms override nnnn ms</b> .                                                                                                                                                                                | <b>detail</b>   |

## Sample Output

### show pim snooping neighbors

```

user@host> show pim snooping neighbors
B = Bidirectional Capable, G = Generation Identifier,
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit

Instance: vpls1
Learning-Domain: vlan-id 10

Interface Option Uptime Neighbor addr
ge-1/3/1.10 HPLGT 00:43:33 192.0.2.2

```

```
ge-1/3/3.10 HPLGT 00:43:33 192.0.2.3
ge-1/3/5.10 HPLGT 00:43:33 192.0.2.4
ge-1/3/7.10 HPLGT 00:43:33 192.0.2.5
```

Learning-Domain: vlan-id 20

```
Interface Option Uptime Neighbor addr
ge-1/3/1.20 HPLGT 00:43:33 192.0.2.12
ge-1/3/3.20 HPLGT 00:43:33 192.0.2.13
ge-1/3/5.20 HPLGT 00:43:33 192.0.2.14
ge-1/3/7.20 HPLGT 00:43:33 192.0.2.15
```

### show pim snooping neighbors detail

```
user@host> show pim snooping neighbors detail
```

Instance: vpls1

Learning-Domain: vlan-id 10

```
Interface: ge-1/3/1.10
Address: 192.0.2.2
Uptime: 00:44:51
Hello Option Holdtime: 105 seconds 83 remaining
Hello Option DR Priority: 1
Hello Option Generation ID: 830908833
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Tracking is supported
```

```
Interface: ge-1/3/3.10
Address: 192.0.2.3
Uptime: 00:44:51
Hello Option Holdtime: 105 seconds 97 remaining
Hello Option DR Priority: 1
Hello Option Generation ID: 2056520742
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Tracking is supported
```

```
Interface: ge-1/3/5.10
Address: 192.0.2.4
Uptime: 00:44:51
Hello Option Holdtime: 105 seconds 81 remaining
Hello Option DR Priority: 1
Hello Option Generation ID: 1152066227
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Tracking is supported
```

```
Interface: ge-1/3/7.10
Address: 192.0.2.5
Uptime: 00:44:51
Hello Option Holdtime: 105 seconds 96 remaining
Hello Option DR Priority: 1
Hello Option Generation ID: 1113200338
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Tracking is supported
Learning-Domain: vlan-id 20
```

```
Interface: ge-1/3/1.20
Address: 192.0.2.12
Uptime: 00:44:51
Hello Option Holdtime: 105 seconds 81 remaining
Hello Option DR Priority: 1
Hello Option Generation ID: 963205167
```



```
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Tracking is supported
```

```
Interface: ge-1/3/3.20
Address: 192.0.2.13
Uptime: 00:44:51
Hello Option Holdtime: 105 seconds 104 remaining
Hello Option DR Priority: 1
Hello Option Generation ID: 166921538
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Tracking is supported
```

```
Interface: ge-1/3/5.20
Address: 192.0.2.14
Uptime: 00:44:51
Hello Option Holdtime: 105 seconds 88 remaining
Hello Option DR Priority: 1
Hello Option Generation ID: 789422835
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Tracking is supported
```

```
Interface: ge-1/3/7.20
Address: 192.0.2.15
Uptime: 00:44:51
Hello Option Holdtime: 105 seconds 88 remaining
Hello Option DR Priority: 1
Hello Option Generation ID: 1563649680
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Tracking is supported
```

### show pim snooping neighbors instance

```
user@host> show pim snooping neighbors instance vpls1
B = Bidirectional Capable, G = Generation Identifier,
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit
```

```
Instance: vpls1
Learning-Domain: vlan-id 10
```

```
Interface Option Uptime Neighbor addr
ge-1/3/1.10 HPLGT 00:46:03 192.0.2.2
ge-1/3/3.10 HPLGT 00:46:03 192.0.2.3
ge-1/3/5.10 HPLGT 00:46:03 192.0.2.4
ge-1/3/7.10 HPLGT 00:46:03 192.0.2.5
```

```
Learning-Domain: vlan-id 20
```

```
Interface Option Uptime Neighbor addr
ge-1/3/1.20 HPLGT 00:46:03 192.0.2.12
ge-1/3/3.20 HPLGT 00:46:03 192.0.2.13
ge-1/3/5.20 HPLGT 00:46:03 192.0.2.14
ge-1/3/7.20 HPLGT 00:46:03 192.0.2.15
```

### show pim snooping neighbors interface

```
user@host> show pim snooping neighbors interface ge-1/3/1.20
B = Bidirectional Capable, G = Generation Identifier,
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit
```

```
Instance: vpls1
Learning-Domain: vlan-id 10
Learning-Domain: vlan-id 20

Interface Option Uptime Neighbor addr
ge-1/3/1.20 HPLGT 00:48:04 192.0.2.12
```

#### show pim snooping neighbors vlan-id

```
user@host> show pim snooping neighbors vlan-id 10
B = Bidirectional Capable, G = Generation Identifier,
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit

Instance: vpls1
Learning-Domain: vlan-id 10

Interface Option Uptime Neighbor addr
ge-1/3/1.10 HPLGT 00:49:12 192.0.2.2
ge-1/3/3.10 HPLGT 00:49:12 192.0.2.3
ge-1/3/5.10 HPLGT 00:49:12 192.0.2.4
ge-1/3/7.10 HPLGT 00:49:12 192.0.2.5
```

## show pim snooping statistics

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show pim snooping statistics<br><instance <i>instance-name</i> ><br><interface <i>interface-name</i> ><br><logical-system <i>logical-system-name</i> ><br><vlan-id <i>vlan-id</i> >                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | Command introduced in Junos OS Release 12.3 for MX Series 3D Universal Edge devices.<br>Command introduced in Junos OS Release 13.2 for M Series Multiservice Edge devices.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | Display Protocol Independent Multicast (PIM) snooping statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                  | <p><b>none</b>—Display PIM statistics.</p> <p><b>instance <i>instance-name</i></b>—(Optional) Display statistics for a specific routing instance enabled by Protocol Independent Multicast (PIM) snooping.</p> <p><b>interface <i>interface-name</i></b>—(Optional) Display statistics about the specified interface for PIM snooping.</p> <p><b>logical-system <i>logical-system-name</i></b>—(Optional) Display information about a particular logical system, or type 'all'.</p> <p><b>vlan-id <i>vlan-identifier</i></b>—(Optional) Display PIM snooping statistics information for the specified VLAN.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>PIM Snooping for VPLS</i></li> <li>• <a href="#">clear pim snooping statistics on page 1237</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>List of Sample Output</b>    | <a href="#">show pim snooping statistics on page 1288</a><br><a href="#">show pim snooping statistics instance on page 1289</a><br><a href="#">show pim snooping statistics interface on page 1290</a><br><a href="#">show pim snooping statistics vlan-id on page 1290</a>                                                                                                                                                                                                                                                                                                                                     |
| <b>Output Fields</b>            | <a href="#">Table 31 on page 1287</a> lists the output fields for the <b>show pim snooping statistics</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                      |

**Table 31: show pim snooping statistics Output Fields**

| Field Name      | Field Description                               | Level of Output |
|-----------------|-------------------------------------------------|-----------------|
| Instance        | Routing instance for PIM snooping.              | All levels      |
| Learning-Domain | Learning domain for PIM snooping.               | All levels      |
| Tx J/P messages | Total number of transmitted join/prune packets. | All levels      |

Table 31: show pim snooping statistics Output Fields (*continued*)

| Field Name                          | Field Description                                                                 | Level of Output |
|-------------------------------------|-----------------------------------------------------------------------------------|-----------------|
| <b>Rx J/P messages</b>              | Total number of received join/prune packets.                                      | All levels      |
| <b>Rx J/P messages -- seen</b>      | Number of join/prune packets seen but not received on the upstream interface.     | All levels      |
| <b>Rx J/P messages -- received</b>  | Number of join/prune packets received on the downstream interface.                | All levels      |
| <b>Rx Hello messages</b>            | Total number of received hello packets.                                           | All levels      |
| <b>Rx Version Unknown</b>           | Number of packets received with an unknown version number.                        | All levels      |
| <b>Rx Neighbor Unknown</b>          | Number of packets received from an unknown neighbor.                              | All levels      |
| <b>Rx Upstream Neighbor Unknown</b> | Number of packets received with unknown upstream neighbor information.            | All levels      |
| <b>Rx Bad Length</b>                | Number of packets received containing incorrect length information.               | All levels      |
| <b>Rx J/P Busy Drop</b>             | Number of join/prune packets dropped while the router is busy.                    | All levels      |
| <b>Rx J/P Group Aggregate 0</b>     | Number of join/prune packets received containing the aggregate group information. | All levels      |
| <b>Rx Malformed Packet</b>          | Number of malformed packets received.                                             | All levels      |
| <b>Rx No PIM Interface</b>          | Number of packets received without the interface information.                     | All levels      |
| <b>Rx No Upstream Neighbor</b>      | Number of packets received without upstream neighbor information.                 | All levels      |
| <b>Rx Unknown Hello Option</b>      | Number of hello packets received with unknown options.                            | All levels      |

## Sample Output

### show pim snooping statistics

```

user@host> show pim snooping statistics
Instance: vpls1
Learning-Domain: vlan-id 10

Tx J/P messages 0
Rx J/P messages 8
Rx J/P messages -- seen 0
Rx J/P messages -- received 8
Rx Hello messages 37

```

```

Rx Version Unknown 0
Rx Neighbor Unknown 0
Rx Upstream Neighbor Unknown 0
Rx Bad Length 0
Rx J/P Busy Drop 0
Rx J/P Group Aggregate 0
Rx Malformed Packet 0
Rx No PIM Interface 0
Rx No Upstream Neighbor 0
Rx Bad Length 0
Rx Neighbor Unknown 0
Rx Unknown Hello Option 0
Rx Malformed Packet 0

```

Learning-Domain: vlan-id 20

```

Tx J/P messages 0
RX J/P messages 2
Rx J/P messages -- seen 0
Rx J/P messages -- received 2
Rx Hello messages 39
Rx Version Unknown 0
Rx Neighbor Unknown 0
Rx Upstream Neighbor Unknown 0
Rx Bad Length 0
Rx J/P Busy Drop 0
Rx J/P Group Aggregate 0
Rx Malformed Packet 0
Rx No PIM Interface 0
Rx No Upstream Neighbor 0
Rx Bad Length 0
Rx Neighbor Unknown 0
Rx Unknown Hello Option 0
Rx Malformed Packet 0

```

### show pim snooping statistics instance

```

user@host> show pim snooping statistics instance vpls1
Instance: vpls1
Learning-Domain: vlan-id 10

```

```

Tx J/P messages 0
RX J/P messages 9
Rx J/P messages -- seen 0
Rx J/P messages -- received 9
Rx Hello messages 45
Rx Version Unknown 0
Rx Neighbor Unknown 0
Rx Upstream Neighbor Unknown 0
Rx Bad Length 0
Rx J/P Busy Drop 0
Rx J/P Group Aggregate 0
Rx Malformed Packet 0
Rx No PIM Interface 0
Rx No Upstream Neighbor 0
Rx Bad Length 0
Rx Neighbor Unknown 0
Rx Unknown Hello Option 0
Rx Malformed Packet 0

```

```
Learning-Domain: vlan-id 20

Tx J/P messages 0
RX J/P messages 3
Rx J/P messages -- seen 0
Rx J/P messages -- received 3
Rx Hello messages 47
Rx Version Unknown 0
Rx Neighbor Unknown 0
Rx Upstream Neighbor Unknown 0
Rx Bad Length 0
Rx J/P Busy Drop 0
Rx J/P Group Aggregate 0
Rx Malformed Packet 0
Rx No PIM Interface 0
Rx No Upstream Neighbor 0
Rx Bad Length 0
Rx Neighbor Unknown 0
Rx Unknown Hello Option 0
Rx Malformed Packet 0
```

#### show pim snooping statistics interface

```
user@host> show pim snooping statistics interface ge-1/3/1.20
Instance: vpls1
Learning-Domain: vlan-id 10
Learning-Domain: vlan-id 20

PIM Interface statistics for ge-1/3/1.20
Tx J/P messages 0
RX J/P messages 0
Rx J/P messages -- seen 0
Rx J/P messages -- received 0
Rx Hello messages 13
Rx Version Unknown 0
Rx Neighbor Unknown 0
Rx Upstream Neighbor Unknown 0
Rx Bad Length 0
Rx J/P Busy Drop 0
Rx J/P Group Aggregate 0
Rx Malformed Packet 0
```

#### show pim snooping statistics vlan-id

```
user@host> show pim snooping statistics vlan-id 10
Instance: vpls1
Learning-Domain: vlan-id 10

Tx J/P messages 0
RX J/P messages 11
Rx J/P messages -- seen 0
Rx J/P messages -- received 11
Rx Hello messages 64
Rx Version Unknown 0
Rx Neighbor Unknown 0
Rx Upstream Neighbor Unknown 0
Rx Bad Length 0
Rx J/P Busy Drop 0
Rx J/P Group Aggregate 0
Rx Malformed Packet 0
```

```
Rx No PIM Interface 0
Rx No Upstream Neighbor 0
Rx Bad Length 0
Rx Neighbor Unknown 0
```

## show route

---

**List of Syntax**   [Syntax on page 1292](#)  
                          [Syntax \(EX Series Switches\) on page 1292](#)

**Syntax**   `show route`  
              `<all>`  
              `<destination-prefix>`  
              `<logical-system (all | logical-system-name)>`  
              `<private>`

**Syntax (EX Series Switches)**   `show route`  
                                      `<all>`  
                                      `<destination-prefix>`  
                                      `<private>`

**Release Information**   Command introduced before Junos OS Release 7.4.  
                              Command introduced in Junos OS Release 9.0 for EX Series switches.  
                              Option **private** introduced in Junos OS Release 9.5.  
                              Option **private** introduced in Junos OS Release 9.5 for EX Series switches.  
                              Command introduced in Junos OS Release 15.1R3 on MX Series routers for enhanced subscriber management.

**Description**   Display the active entries in the routing tables.

**Options**   **none**—Display brief information about all active entries in the routing tables.

**all**—(Optional) Display information about all routing tables, including private, or internal, routing tables.

**destination-prefix**—(Optional) Display active entries for the specified address or range of addresses.

**logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**private**—(Optional) Display information only about all private, or internal, routing tables.

**Required Privilege Level**   view

**Related Documentation**

- *Example: Configuring RIP*
- *Examples: Configuring Internal BGP Peering*
- *Examples: Configuring External BGP Peering*
- *Examples: Configuring OSPF Routing Policy*
- *Verifying and Managing Junos OS Enhanced Subscriber Management*

**List of Sample Output**   [show route on page 1295](#)  
                                  [show route on page 1296](#)



[show route \(with Destination Prefix\) on page 1296](#)  
[show route destination-prefix detail on page 1296](#)  
[show route extensive on page 1297](#)  
[show route \(Enhanced Subscriber Management\) on page 1297](#)

**Output Fields** Table 32 on page 1293 describes the output fields for the **show route** command. Output fields are listed in the approximate order in which they appear.

**Table 32: show route Output Fields**

| Field Name                 | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>routing-table-name</i>  | Name of the routing table (for example, inet.0).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <i>number destinations</i> | Number of destinations for which there are routes in the routing table.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <i>number routes</i>       | <p>Number of routes in the routing table and total number of routes in the following states:</p> <ul style="list-style-type: none"> <li>• <b>active</b> (routes that are active).</li> <li>• <b>holddown</b> (routes that are in the pending state before being declared inactive). A holddown route was once the active route and is no longer the active route. The route is in the holddown state because a protocol still has interest in the route, meaning that the interest bit is set. A protocol might have its interest bit set on the previously active route because the protocol is still advertising the route. The route will be deleted after all protocols withdraw their advertisement of the route and remove their interest bit. A persistent holddown state often means that the interested protocol is not releasing its interest bit properly.</li> </ul> <p>However, if you have configured advertisement of multiple routes (with the <b>add-path</b> or <b>advertise-inactive</b> statement), the holddown bit is most likely set because BGP is advertising the route as an active route. In this case, you can ignore the holddown state because nothing is wrong.</p> <ul style="list-style-type: none"> <li>• <b>hidden</b> (routes that are not used because of a routing policy).</li> </ul> |
| <i>destination-prefix</i>  | <p>Route destination (for example: 10.0.0.1/24). Sometimes the route information is presented in another format, such as:</p> <ul style="list-style-type: none"> <li>• <b>MPLS-label</b> (for example, 80001).</li> <li>• <b>interface-name</b> (for example, ge-1/0/2).</li> <li>• <b>neighbor-address:control-word-status:encapsulation type:vc-id:source</b> (Layer 2 circuit only. For example, 10.1.1.195:NoCtrlWord:1:1:Local/96): <ul style="list-style-type: none"> <li>• <b>neighbor-address</b>—Address of the neighbor.</li> <li>• <b>control-word-status</b>—Whether the use of the control word has been negotiated for this virtual circuit: <b>NoCtrlWord</b> or <b>CtrlWord</b>.</li> <li>• <b>encapsulation type</b>—Type of encapsulation, represented by a number: (1) Frame Relay DLCI, (2) ATM AAL5 VCC transport, (3) ATM transparent cell transport, (4) Ethernet, (5) VLAN Ethernet, (6) HDLC, (7) PPP, (8) ATM VCC cell transport, (10) ATM VPC cell transport.</li> <li>• <b>vc-id</b>—Virtual circuit identifier.</li> <li>• <b>source</b>—Source of the advertisement: <b>Local</b> or <b>Remote</b>.</li> </ul> </li> </ul>                                                                                                                                                                     |

Table 32: show route Output Fields (*continued*)

| Field Name                                        | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ <i>protocol, preference</i> ]                   | <p>Protocol from which the route was learned and the preference value for the route.</p> <ul style="list-style-type: none"> <li>• +—A plus sign indicates the active route, which is the route installed from the routing table into the forwarding table.</li> <li>• - —A hyphen indicates the last active route.</li> <li>• *—An asterisk indicates that the route is both the active and the last active route. An asterisk before a <b>to</b> line indicates the best subpath to the route.</li> </ul> <p>In every routing metric except for the BGP <b>LocalPref</b> attribute, a lesser value is preferred. In order to use common comparison routines, Junos OS stores the 1's complement of the <b>LocalPref</b> value in the <b>Preference2</b> field. For example, if the <b>LocalPref</b> value for Route 1 is 100, the <b>Preference2</b> value is -101. If the <b>LocalPref</b> value for Route 2 is 155, the <b>Preference2</b> value is -156. Route 2 is preferred because it has a higher <b>LocalPref</b> value and a lower <b>Preference2</b> value.</p>                                                                                                                                                                                                                                   |
| <i>weeks:days</i><br><i>hours:minutes:seconds</i> | How long the route been known (for example, <b>2w4d 13:11:14</b> , or 2 weeks, 4 days, 13 hours, 11 minutes, and 14 seconds).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| metric                                            | Cost value of the indicated route. For routes within an AS, the cost is determined by the IGP and the individual protocol metrics. For external routes, destinations, or routing domains, the cost is determined by a preference value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| localpref                                         | Local preference value included in the route.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| from                                              | Interface from which the route was received.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| AS path                                           | <p>AS path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated:</p> <ul style="list-style-type: none"> <li>• I—IGP.</li> <li>• E—EGP.</li> <li>• ?—Incomplete; typically, the AS path was aggregated.</li> </ul> <p>When AS path numbers are included in the route, the format is as follows:</p> <ul style="list-style-type: none"> <li>• [ ]—Brackets enclose the local AS number associated with the AS path if more than one AS number is configured on the routing device, or if AS path prepending is configured.</li> <li>• { }—Braces enclose AS sets, which are groups of AS numbers in which the order does not matter. A set commonly results from route aggregation. The numbers in each AS set are displayed in ascending order.</li> <li>• ( )—Parentheses enclose a confederation.</li> <li>• ( [ ] )—Parentheses and brackets enclose a confederation set.</li> </ul> <p><b>NOTE:</b> In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance.</p> |

Table 32: show route Output Fields (*continued*)

| Field Name              | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>validation-state</b> | <p>(BGP-learned routes) Validation status of the route:</p> <ul style="list-style-type: none"> <li>• <b>Invalid</b>—Indicates that the prefix is found, but either the corresponding AS received from the EBGP peer is not the AS that appears in the database, or the prefix length in the BGP update message is longer than the maximum length permitted in the database.</li> <li>• <b>Unknown</b>—Indicates that the prefix is not among the prefixes or prefix ranges in the database.</li> <li>• <b>Unverified</b>—Indicates that the origin of the prefix is not verified against the database. This is because the database got populated and the validation is not called for in the BGP import policy, although origin validation is enabled, or the origin validation is not enabled for the BGP peers.</li> <li>• <b>Valid</b>—Indicates that the prefix and autonomous system pair are found in the database.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>to</b>               | <p>Next hop to the destination. An angle bracket (&gt;) indicates that the route is the selected route.</p> <p>If the destination is <b>Discard</b>, traffic is dropped.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>via</b>              | <p>Interface used to reach the next hop. If there is more than one interface available to the next hop, the interface that is actually used is followed by the word <b>Selected</b>. This field can also contain the following information:</p> <ul style="list-style-type: none"> <li>• <b>Weight</b>—Value used to distinguish primary, secondary, and fast reroute backup routes. Weight information is available when MPLS label-switched path (LSP) link protection, node-link protection, or fast reroute is enabled, or when the standby state is enabled for secondary paths. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible.</li> <li>• <b>Balance</b>—Balance coefficient indicating how traffic of unequal cost is distributed among next hops when a routing device is performing unequal-cost load balancing. This information is available when you enable BGP multipath load balancing.</li> <li>• <b>lsp-path-name</b>—Name of the LSP used to reach the next hop.</li> <li>• <b>label-action</b>—MPLS label and operation occurring at the next hop. The operation can be <b>pop</b> (where a label is removed from the top of the stack), <b>push</b> (where another label is added to the label stack), or <b>swap</b> (where a label is replaced by another label). For VPNs, expect to see multiple <b>push</b> operations, corresponding to the inner and outer labels required for VPN routes (in the case of a direct PE-to-PE connection, the VPN route would have the inner label push only).</li> </ul> |
| <b>Private unicast</b>  | <p>(Enhanced subscriber management for MX Series routers) Indicates that an access-internal route is managed by enhanced subscriber management. By contrast, access-internal routes <i>not</i> managed by enhanced subscriber management are displayed with associated next-hop and media access control (MAC) address information.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Sample Output

### show route

```

user@host> show route
inet.0: 11 destinations, 12 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1:65500:1:10.0.0.20/240
 * [MVPN/70] 19:53:41, metric2 1
 Indirect
1:65500:1:10.0.0.40/240
 * [BGP/170] 19:53:29, localpref 100, from 10.0.0.30
 AS path: I
 > to 10.0.24.4 via 1t-0/3/0.24, label-switched-path toD

```

```

[BGP/170] 19:53:26, localpref 100, from 10.0.0.33
AS path: I
> to 10.0.24.4 via lt-0/3/0.24, label-switched-path toD
1:65500:1:10.0.0.60/240
*[BGP/170] 19:53:29, localpref 100, from 10.0.0.30
AS path: I
> to 10.0.28.8 via lt-0/3/0.28, label-switched-path toF
[BGP/170] 19:53:25, localpref 100, from 10.0.0.33
AS path: I
> to 10.0.28.8 via lt-0/3/0.28, label-switched-path toF

```

### show route

The following sample output shows a VPN route with composite next hops enabled. The first **Push** operation corresponds to the outer label. The second **Push** operation corresponds to the inner label.

```

user@host> show route 192.0.2.0

13979:665001.inet.0: 871 destinations, 3556 routes (871 active, 0 holddown, 0
hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.0/24 @[BGP/170] 00:28:32, localpref 100, from 10.9.9.160
 AS path: 13980 ?, validation-state: unverified
 > to 10.100.0.42 via ae2.0, Push 16, Push 300368(top)
 [BGP/170] 00:28:28, localpref 100, from 10.9.9.169
 AS path: 13980 ?, validation-state: unverified
 > to 10.100.0.42 via ae2.0, Push 126016, Push 300368(top)
 #[Multipath/255] 00:28:28, metric2 102
 > to 10.100.0.42 via ae2.0, Push 16, Push 300368(top)
 to 10.100.0.42 via ae2.0, Push 16, Push 300368(top)

```

### show route (with Destination Prefix)

```

user@host> show route 172.16.0.0/12

inet.0: 10 destinations, 10 routes (9 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.0.0/12 *[Static/5] 2w4d 12:54:27
 > to 192.168.167.254 via fxp0.0

```

### show route destination-prefix detail

```

user@host> show route 198.51.100.0 detail

inet.0: 15 destinations, 20 routes (15 active, 0 holddown, 0 hidden)
198.51.100.0/24 (2 entries, 2 announced)
 *BGP Preference: 170/-101
 ...
 BGP-Static Preference: 4294967292
 Next hop type: Discard
 Address: 0x9041ae4
 Next-hop reference count: 2
 State: <NoReadvrt Int Ext AlwaysFlash>
 Inactive reason: Route Preference
 Local AS: 200
 Age: 4d 1:40:40
 Validation State: unverified
 Task: RT

```

```
Announcement bits (1): 2-BGP_RT_Background
AS path: 4 5 6 I
```

### show route extensive

```
user@host> show route extensive
v1.mvpn.0: 5 destinations, 8 routes (5 active, 1 holddown, 0 hidden)
1:65500:1:10.0.0.40/240 (1 entry, 1 announced)
 *BGP Preference: 170/-101
 PMSI: Flags 0x0: Label[0:0:0]: PIM-SM: Sender 10.0.0.40 Group
203.0.113.1
 Next hop type: Indirect
 Address: 0x92455b8
 Next-hop reference count: 2
 Source: 10.0.0.30
 Protocol next hop: 10.0.0.40
 Indirect next hop: 2 no-forward
 State: <Active Int Ext>
 Local AS: 65500 Peer AS: 65500
 Age: 3 Metric2: 1
 Validation State: unverified
 Task: BGP_65500.10.0.0.30+179
 Announcement bits (2): 0-PIM.v1 1-mvpn global task
 AS path: I (Originator) Cluster list: 10.0.0.30
 AS path: Originator ID: 10.0.0.40
 Communities: target:65520:100
 Import Accepted
 Localpref: 100
 Router ID: 10.0.0.30
 Primary Routing Table bgp.mvpn.0
 Indirect next hops: 1
 Protocol next hop: 10.0.0.40 Metric: 1
 Indirect next hop: 2 no-forward
 Indirect path forwarding next hops: 1
 Next hop type: Router
 Next hop: 10.0.24.4 via lt-0/3/0.24 weight 0x1
 10.0.0.40/32 Originating RIB: inet.3
 Metric: 1 Node path count: 1
 Forwarding nexthops: 1
 Nexthop: 10.0.24.4 via lt-0/3/0.24
```

### show route (Enhanced Subscriber Management)

```
user@host> show route
inet.0: 41 destinations, 41 routes (40 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

198.51.100.11/32 *[Access-internal/12] 00:00:08
> to #0 10.0.0.1.93.65 via demux0.1073741824
198.51.100.12/32 *[Access-internal/12] 00:00:08
 Private unicast
.
.
.
```

## show security group-vpn member ike security-associations

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show security group-vpn member ike security-associations [brief   detail] [index <i>sa-index</i> ] [ <i>peer-ipaddress</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | Display IKE security associations (SAs) for group members.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li>• <b>none</b>—Display summary information about all IKE SAs for the group members.</li> <li>• <b>brief</b>—(Optional) Display summary output.</li> <li>• <b>detail</b>—(Optional) Display detailed output.</li> <li>• <b>index <i>sa-index</i></b>—(Optional) Display detailed information about the specified SA identified by index number. To obtain a list of all SAs that includes their index numbers, use the command with no options.</li> <li>• <b>peer-ipaddress</b>—(Optional) Display information about the SA with the specified peer.</li> </ul> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear security group-vpn member ike security-associations on page 1239</a></li> <li>• <a href="#">Group VPNv2 Overview</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>List of Sample Output</b>    | <a href="#">show security group-vpn member ike security-associations on page 1300</a><br><a href="#">show security group-vpn member ike security-associations detail on page 1300</a>                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Output Fields</b>            | Table 33 on page 1298 lists the output fields for the <b>show security group-vpn member ike security-associations</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                |

**Table 33: show security group-vpn member ike security-associations Output Fields**

| Field Name              | Field Description                                                                                                                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Index</b>            | Index number of an SA. This number is an internally generated number you can use to display information about a single SA.                                                                                   |
| <b>State</b>            | State of the IKE security associations: <ul style="list-style-type: none"> <li>• <b>DOWN</b>—SA has not been negotiated with the peer.</li> <li>• <b>UP</b>—SA has been negotiated with the peer.</li> </ul> |
| <b>Initiator cookie</b> | Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.                                                                                                      |

Table 33: show security group-vpn member ike security-associations Output Fields (*continued*)

| Field Name                   | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Responder cookie</b>      | <p>Random number generated by the remote node and sent back to the initiator as a verification that the packets were received.</p> <p>A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Mode</b>                  | <p>Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between themselves. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are</p> <ul style="list-style-type: none"> <li>• <b>main</b>—The exchange is done with six messages. This mode or exchange type encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate.</li> <li>• <b>aggressive</b>—The exchange is done with three messages. This mode or exchange type does not encrypt the payload, leaving the identity of the neighbor unprotected.</li> </ul>        |
| <b>Remote Address</b>        | IP address of the destination peer with which the local peer communicates.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>IKE Peer</b>              | IP address of the destination peer with which the local peer communicates.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Exchange type</b>         | <p>Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between themselves. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are</p> <ul style="list-style-type: none"> <li>• <b>main</b>—The exchange is done with six messages. This mode or exchange type encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate.</li> <li>• <b>aggressive</b>—The exchange is done with three messages. This mode or exchange type does not encrypt the payload, leaving the identity of the neighbor unprotected.</li> </ul>        |
| <b>Authentication method</b> | <p>Method the server uses to authenticate the source of IKE messages:</p> <ul style="list-style-type: none"> <li>• <b>pre-shared-keys</b>—Preshared key for encryption and decryption that both participants must have before beginning tunnel negotiations.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Local</b>                 | Address of the local peer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Lifetime</b>              | Number of seconds remaining until the IKE SA expires.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Algorithms</b>            | <p>Internet Key Exchange (IKE) algorithms used to encrypt and secure exchanges between the peers during the IPsec Phase 2 process:</p> <ul style="list-style-type: none"> <li>• <b>Authentication</b>—Type of authentication algorithm used. <ul style="list-style-type: none"> <li>• <b>sha-256</b>—Secure Hash Algorithm 256 authentication.</li> <li>• <b>sha-384</b>—Secure Hash Algorithm 384 authentication.</li> </ul> </li> <li>• <b>Encryption</b>—Type of encryption algorithm used. <ul style="list-style-type: none"> <li>• <b>aes-256-cbc</b>—Advanced Encryption Standard (AES) 256-bit encryption.</li> <li>• <b>aes-192-cbc</b>—AES192-bit encryption</li> <li>• <b>aes-128-cbc</b>—AES 128-bit encryption.</li> </ul> </li> </ul> |

Table 33: show security group-vpn member ike security-associations Output Fields (*continued*)

| Field Name         | Field Description                                                                                                                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Traffic statistics | <ul style="list-style-type: none"> <li>• <b>Input bytes</b>—Number of bytes received.</li> <li>• <b>Output bytes</b>—Number of bytes transmitted.</li> <li>• <b>Input packets</b>—Number of packets received.</li> <li>• <b>Output packets</b>—Number of packets transmitted.</li> </ul> |

## Sample Output

### show security group-vpn member ike security-associations

```

user@host> show security group-vpn member ike security-associations
Index State Initiator cookie Responder cookie Mode Remote Address

4736345 UP 70611c65603d53da 6e0888777ad10f8d Main 192.168.1.53

```

## Sample Output

### show security group-vpn member ike security-associations detail

```

user@host> show security group-vpn member ike security-associations detail
IKE peer 192.168.2.53, Index 5824842, Gateway Name: group1_2
 Role: Initiator, State: UP
 Initiator cookie: fc866556b8afe4cd, Responder cookie: 1238de6b8a89de44
 Exchange type: Main, Authentication method: Pre-shared-keys
 Local: 192.168.2.170:848, Remote: 192.168.2.53:848
 Lifetime: Expires in 2 seconds
 Peer ike-id: 192.168.2.53
 Xauth user-name: not available
 Xauth assigned IP: 0.0.0.0
 Algorithms:
 Authentication : hmac-sha1-96
 Encryption : 3des-cbc
 Pseudo random function: hmac-sha1
 Diffie-Hellman group : DH-group-2
 Traffic statistics:
 Input bytes : 2044
 Output bytes : 900
 Input packets: 7
 Output packets: 7
 Flags: IKE SA is created

```



## show security group-vpn member kek security-associations

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show security group-vpn member kek security-associations [brief   detail   display xml] [index sa-index] [peer-ipaddress]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Display Group VPNv2 security associations (SAs) for a group member.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li>• <b>none</b>—Display information about all Group VPNv2 SAs for the group member.</li> <li>• <b>brief</b>—(Optional) Display summary output.</li> <li>• <b>detail</b>—(Optional) Display detailed output.</li> <li>• <b>display xml</b>—(Optional) Display xml.</li> <li>• <b>index sa-index</b>—(Optional) Display detailed information about the specified SA identified by index number. To obtain a list of all SAs that includes their index numbers, use the command with no options.</li> <li>• <b>peer-ipaddress</b>—(Optional) Display information about the SA with the specified peer.</li> </ul> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Group VPNv2 Overview</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>List of Sample Output</b>    | <a href="#">show security group-vpn member kek security-associations on page 1303</a><br><a href="#">show security group-vpn member kek security-associations detail on page 1303</a><br><a href="#">show security group-vpn member kek security-associations detail   display xml on page 1303</a>                                                                                                                                                                                                                                                                                                                                                 |
| <b>Output Fields</b>            | Table 34 on page 1301 lists the output fields for the <b>show security group-vpn member kek security-associations</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Table 34: show security group-vpn member kek security-associations

| Field Name              | Field Description                                                                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Index</b>            | Index number of an SA. This number is an internally generated number you can use to display information about a single SA.                                   |
| <b>Remote Address</b>   | IP address of the destination peer with which the local peer communicates.                                                                                   |
| <b>State</b>            | State of the KEK security associations: <ul style="list-style-type: none"> <li>• <b>DOWN</b>—SA is not active.</li> <li>• <b>UP</b>—SA is active.</li> </ul> |
| <b>Initiator cookie</b> | Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.                                                      |

Table 34: show security group-vpn member kek security-associations (*continued*)

| Field Name                        | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Responder cookie</b>           | Random number generated by the remote node and sent back to the initiator as a verification that the packets were received.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>SPI</b>                        | Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>GroupID</b>                    | Group identifier.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>KEK Peer</b>                   | IP address of the destination peer with which the local peer communicates.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Role</b>                       | For the member, it is always responder.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>State</b>                      | State of the KEK security associations, which is always up.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Authentication method</b>      | RSA is the supported authentication method.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Local</b>                      | Address of the local peer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Remote</b>                     | Address of the remote peer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Lifetime</b>                   | Number of seconds remaining until the IKE SA expires.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Algorithms</b>                 | <p>Internet Key Exchange (IKE) algorithms used to encrypt and secure exchanges between the peers during the IPsec Phase 2 process:</p> <ul style="list-style-type: none"> <li>• <b>Sig-hash</b>—Type of authentication algorithm used. <ul style="list-style-type: none"> <li>• <b>sha-256</b>—Secure Hash Algorithm 256 (sha-256) authentication.</li> <li>• <b>sha-384</b>—Secure Hash Algorithm 394 (sha-384) authentication.</li> </ul> </li> <li>• <b>Sig key length (bits)</b>—Size of signature key in bits.</li> <li>• <b>Encryption</b>—Type of encryption algorithm used. <ul style="list-style-type: none"> <li>• <b>aes-256-cbc</b>—Advanced Encryption Standard (AES) 256-bit encryption.</li> <li>• <b>aes-192-cbc</b>—AES192-bit encryption</li> <li>• <b>aes-128-cbc</b>—AES 128-bit encryption.</li> <li>• <b>3des-cbc</b>—3 Data Encryption Standard (DES) encryption.</li> <li>• <b>des-cbc</b>—DES encryption.</li> </ul> </li> </ul> |
| <b>Traffic statistics</b>         | <ul style="list-style-type: none"> <li>• <b>Input bytes</b>—Number of bytes received.</li> <li>• <b>Output bytes</b>—Number of bytes transmitted.</li> <li>• <b>Input packets</b>—Number of packets received.</li> <li>• <b>Output packets</b>—Number of packets transmitted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Server Info Version</b>        | Identify the latest set of information maintained in the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Server Heartbeat Interval</b>  | Interval in seconds at which the server sends heartbeats to group members.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Member Heartbeat Threshold</b> | The heartbeat threshold configured on the group member for the IPsec VPN. If this number of heartbeats is missed on the member, the member reregisters with the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

Table 34: show security group-vpn member kek security-associations (*continued*)

| Field Name                     | Field Description                                                                                                                                                                                              |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Heartbeat Timeout Left         | Number of heartbeats until the heartbeat threshold is reached, at which time the member reregisters with the server.<br><br><b>NOTE:</b> When this number reaches 0, reregistration happens within 60 seconds. |
| Server Activation Delay        | Number of seconds before a group member can use a new key when the member reregisters with the server.                                                                                                         |
| Server Multicast Group         | Multicast IP address to which the server sends rekey messages.                                                                                                                                                 |
| Server Replay Window           | Antireplay time window value in milliseconds. 0 means antireplay is disabled.                                                                                                                                  |
| Group Key Push sequence number | Sequence number of the KEK SA groupkey-push message. This number is incremented with every groupkey-push message.                                                                                              |

## Sample Output

### show security group-vpn member kek security-associations

```

user@host> show security group-vpn member kek security-associations
Index Server Address Life:sec Initiator cookie Responder cookie GroupId
5824843 192.168.2.53 166 46871e26227f08f3 f0a463a4d5c3737b 1

```

## Sample Output

### show security group-vpn member kek security-associations detail

```

user@host> show security group-vpn member kek security-associations detail
Index 5824843, Group Id: 1
Group VPN Name: group1_2
Local Gateway: 192.168.2.170, GDOI Server: 192.168.2.53
Initiator cookie: 46871e26227f08f3, Responder cookie: f0a463a4d5c3737b
Lifetime: Expires in 155 seconds
Group Key Push Sequence number: 0

```

```

Algorithms:
 Sig-hash : hmac-md5-96
 Encryption : 3des-cbc

```

```

Traffic statistics:
 Input bytes : 0
 Output bytes : 0
 Input packets: 0
 Output packets: 0

```

```

Stats:
 Push received : 0
 Delete received : 0

```

### show security group-vpn member kek security-associations detail | display xml

```

user@host> show security group-vpn member kek security-associations detail | display xml

```

```

<rpc-reply xmlns:junos="http://xml.example.net/junos/15.1/junos">
 <gvpn-kek-security-associations-information junos:style="detail">
 <kek-security-associations-block>

```

```

 <security-association-index>2987691</security-association-index>
 <group-id>400</group-id>
 <group-vpn-name>gvpn400</group-vpn-name>
 <local-address>192.168.1.100</local-address>
 <server-address>192.168.1.1</server-address>
 <initiator-cookie>510f854307a03675</initiator-cookie>
 <responder-cookie>690e5f121fba6de7</responder-cookie>
 <lifetime-remaining>Expires in 23729 seconds</lifetime-remaining>
 <push-sequence-number>364</push-sequence-number>
 <ike-security-associations>
 <ike-sa-algorithms>

<ike-sa-authentication-algorithm>hmac-sha1-96</ike-sa-authentication-algorithm>
 <ike-sa-sig-key-length>2048</ike-sa-sig-key-length>

<ike-sa-encryption-algorithm>aes128-cbc</ike-sa-encryption-algorithm>
 </ike-sa-algorithms>
 <ike-sa-traffic-statistics>
 <ike-sa-input-bytes>3012</ike-sa-input-bytes>
 <ike-sa-output-bytes>252</ike-sa-output-bytes>
 <ike-sa-input-packets>3</ike-sa-input-packets>
 <ike-sa-output-packets>3</ike-sa-output-packets>
 </ike-sa-traffic-statistics>
 </ike-security-associations>
 <gvpn-kek-security-association-statistics>
 <kek-security-association-statistics> Push received
: 3</kek-security-association-statistics>
 <kek-security-association-statistics> Delete received
: 0</kek-security-association-statistics>
 </gvpn-kek-security-association-statistics>
 </kek-security-associations-block>
 </gvpn-kek-security-associations-information>
 </cli>
 <banner></banner>
</cli>
</rpc-reply>

```

## show vpls connections

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>show vpls connections &lt;brief   extensive&gt; &lt;down   up   up-down&gt; &lt;history&gt; &lt;instance <i>instance-name</i> local-site <i>local-site-name</i> remote-site <i>remote-site-name</i>&gt; &lt;instance-history&gt; &lt;logical-system (all   <i>logical-system-name</i>)&gt; &lt;status&gt; &lt;summary&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | <p>Command introduced before Junos OS Release 7.4.</p> <p><b>instance-history</b> option introduced in Junos OS Release 12.3R2.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | (T Series and M Series routers, except for the M160 router) Display virtual private LAN service (VPLS) connection information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Options</b>                  | <p><b>none</b>—Display information about all VPLS connections for all routing instances.</p> <p><b>brief   extensive</b>—(Optional) Display the specified level of output.</p> <p><b>down   up   up-down</b>—(Optional) Display nonoperational, operational, or both types of connections.</p> <p><b>history</b>—(Optional) Display information about connection history.</p> <p><b>instance <i>instance-name</i></b>—(Optional) Display the VPLS connections for the specified routing instance only.</p> <p><b>instance-history</b>—(Optional) Display information about connection history for a particular instance.</p> <p><b>local-site <i>local-site-name</i></b>—(Optional) Display the VPLS connections for the specified local site name or ID only.</p> <p><b>remote-site <i>remote-site-name</i></b>—(Optional) Display the VPLS connections for the specified remote site name or ID only. Label block size information is always shown as 0 when using this option.</p> <p><b>logical-system (all   <i>logical-system-name</i>)</b>—(Optional) Perform this operation on all logical systems or on a particular logical system.</p> <p><b>status</b>—(Optional) Display information about the connection and interface status.</p> <p><b>summary</b>—(Optional) Display summary of all VPLS connections information.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>List of Sample Output</b>    | <p><a href="#">show vpls connections on page 1310</a></p> <p><a href="#">show vpls connections (with multiple pseudowires) on page 1312</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

[show vpls connections extensive \(Static VPLS Neighbors\) on page 1313](#)

**Output Fields** [Table 35 on page 1306](#) lists the output fields for the **show vpls connections** command. Output fields are listed in the approximate order in which they appear.

**Table 35: show vpls connections Output Fields**

| Field Name                           | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Instance</b>                      | Name of the VPLS instance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Local site</b>                    | Name of the local site.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>VPLS-id</b>                       | Identifier for the VPLS site.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Number of local interfaces</b>    | Number of interfaces configured for the local site.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Number of local interfaces up</b> | Number of interfaces configured for the local site that are currently up.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>IRB interface present</b>         | Indicates whether or not an integrated routing and bridging (IRB) interface is present ( <b>yes</b> or <b>no</b> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Intf</b>                          | <p>List of all of the interfaces configured for the local site. The types of interfaces can include VPLS virtual loopback tunnel interfaces and label-switched interfaces. Any interface that supports VPLS could be listed here.</p> <p>Virtual loopback tunnel interfaces are displayed using the <b>vt-fpc/pic/port.nnnnn</b> format. Label-switched interfaces are displayed using the <b>lsi.nnnnn</b> format. In both cases, <b>nnnnn</b> is a dynamically generated virtual port used to transport and receive packets from other provider edge (PE) routers in the VPLS domain.</p> <p>Each interface might include the following information:</p> <ul style="list-style-type: none"> <li>• Identification as a VPLS interface</li> <li>• Name of the associated VPLS routing instance</li> <li>• Local site number</li> <li>• Remote site number</li> <li>• VPLS neighbor address</li> <li>• VPLS identifier</li> </ul> |
| <b>Interface flags</b>               | <p>Flag associated with the interface. Can include the following:</p> <ul style="list-style-type: none"> <li>• <b>VC-Down</b>—The virtual circuit associated with this interface is down.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Label-base</b>                    | First label in a block of labels. A remote PE router uses this first label when sending traffic toward the advertising PE router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Offset</b>                        | Displays the VPLS Edge (VE) block offset in the Layer 2 VPN NLRI. The VE block offset is used to identify a label block from which a particular label value is selected to setup a pseduowire for a remote site. The block offset value itself indicates the starting VE ID that maps to the label base contained in the VPLS NLRI advertisement.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

Table 35: show vpls connections Output Fields (*continued*)

| Field Name             | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Size</b>            | Label block size. A configurable value that represents the number of label blocks required to cover all the pseudowires for the remote peer. Acceptable configuration values are: <b>2</b> , <b>4</b> , <b>8</b> and <b>16</b> . The default value is <b>2</b> . A value of <b>0</b> will be displayed when using the <b>remote-site</b> option.                                                                                            |
| <b>Range</b>           | Label block range. A value that keeps track of the numbers of remote sites discovered within each label block.                                                                                                                                                                                                                                                                                                                              |
| <b>Preference</b>      | Preference value advertised for a VPLS site. When multiple PE routers are assigned the same VE ID for multihoming, you might need to specify that a particular PE router acts as the designated forwarder by configuring the site preference value. The site preference indicates the degree of preference for a particular customer site. The site preference is one of the tie-breaking criteria used in a designated forwarder election. |
| <b>status-vector</b>   | Bit vector advertising the state of local PE-CE circuits to remote PE routers. A bit value of <b>0</b> indicates that the local circuit and LSP tunnel to the remote PE router are up, whereas a value of <b>1</b> indicates either one or both are down.                                                                                                                                                                                   |
| <b>connection-site</b> | Name of the connection site.                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Neighbor</b>        | IP address and VPLS identifier for the VPLS neighbor. If multiple pseudowires have been configured, the IP address will also show the PW-specific <b>vpls-id-list</b> , for example, 10.255.144.4 (vpls-id 200).                                                                                                                                                                                                                            |
| <b>Type</b>            | Type of connection: <b>loc</b> (local) or <b>rmt</b> (remote).                                                                                                                                                                                                                                                                                                                                                                              |

Table 35: show vpls connections Output Fields (*continued*)

| Field Name | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>St</b>  | <p>Status of the VPLS connection (corresponds with Legend for Connection Status):</p> <ul style="list-style-type: none"> <li>• <b>EI</b>—The local VPLS interface is configured with an encapsulation that is not supported.</li> <li>• <b>EM</b>—The encapsulation type received on this VPLS connection from the neighbor does not match the local VPLS connection interface encapsulation type.</li> <li>• <b>VC-Dn</b>—The virtual circuit is currently down.</li> <li>• <b>CM</b>—The two routers do not agree on a control word, which causes a control word mismatch.</li> <li>• <b>CN</b>—The virtual circuit is not provisioned properly.</li> <li>• <b>OR</b>—The label associated with the virtual circuit is out of range.</li> <li>• <b>OL</b>—No advertisement has been received for this virtual circuit from the neighbor. There is no outgoing label available for use by this virtual circuit.</li> <li>• <b>LD</b>—All of the CE-facing interfaces to the local site are down. Therefore, the connection to the local site is signaled as down to the other PE routers. No pseudowires can be established.</li> <li>• <b>RD</b>—All the interfaces to the remote neighbor are down. Therefore, the remote site has been signaled as down to the other PE routers. No pseudowires can be established.</li> <li>• <b>LN</b>—The local site has lost path selection to the remote site and therefore no pseudowires can be established from this local site.</li> <li>• <b>RN</b>—The remote site has lost path selection to a local site or other remote site and therefore no pseudowires are established to this remote site.<br/>In a multihoming configuration, one multihomed PE site displays the state <b>LN</b>, and the other multihomed PE site displays the state <b>RN</b> in the following circumstances: <ul style="list-style-type: none"> <li>• The multihomed links are both configured to be the backup site.</li> <li>• The two multihomed PE routers have the same site ID, but have a peering relationship with a route reflector (RR) that has a different site ID.</li> </ul> </li> <li>• <b>XX</b>—The VPLS connection is down for an unknown reason. This is a programming error.</li> <li>• <b>MM</b>—The MTU for the local site and the remote site do not match.</li> <li>• <b>BK</b>—The router is using a backup connection.</li> <li>• <b>PF</b>—Profile parse failure.</li> <li>• <b>RS</b>—The remote site is in a standby state.</li> <li>• <b>NC</b>—The interface encapsulation is not configured as an appropriate CCC, TCC, or VPLS encapsulation.</li> <li>• <b>WE</b>—The encapsulation configured for the interface does not match the encapsulation configured for the associated connection within the VPLS routing instance.</li> </ul> |



Table 35: show vpls connections Output Fields (*continued*)

| Field Name           | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | <ul style="list-style-type: none"> <li>• <b>NP</b>—The router detects that interface hardware is not present. The hardware might be offline, a PIC might not be of the desired type, or the interface might be configured in a different routing instance.</li> <li>• <b>--&gt;</b>—Only the outbound connection is up.</li> <li>• <b>&lt;--</b>—Only the inbound connection is up.</li> <li>• <b>Up</b>—The VPLS connection is operational.</li> <li>• <b>Dn</b>—The VPLS connection is down.</li> <li>• <b>CF</b>—The router cannot find enough bandwidth to the remote router to satisfy the VPLS connection bandwidth requirement.</li> <li>• <b>SC</b>—The local site identifier matches the remote site identifier. No pseudowire can be established between these two sites. You should configure different values for the local and remote site identifiers.</li> <li>• <b>LM</b>—The local site identifier is not the minimum designated, meaning it is not the lowest. There is another local site with a lower site identifier. Pseudowires are not being established to this local site, and the associated local site identifier is not being used to distribute VPLS label blocks. However, this is not an error state. Traffic continues to be forwarded to the PE router interfaces connected to the local sites when the local sites are in this state.</li> <li>• <b>RM</b>—The remote site identifier is not the minimum designated, meaning it is not the lowest. There is another remote site connected to the same PE router which has lower site identifier. The PE router cannot establish a pseudowire to this remote site and the associated remote site identifier cannot be used to distribute VPLS label blocks. However, this is not an error state. Traffic can continue to be forwarded to the PE router interface connected to this remote site when the remote site is in this state.</li> <li>• <b>IL</b>—The incoming packets for the VPLS connection have no MPLS label.</li> <li>• <b>MI</b>—The configured mesh group identifier is in use by another system in the network.</li> <li>• <b>ST</b>—The router has switched to a standby connection.</li> <li>• <b>PB</b>—Profile busy.</li> <li>• <b>SN</b>—The VPLS neighbor is static.</li> </ul> |
| <b>Time last up</b>  | Time connection was last in the <b>Up</b> condition.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b># Up trans</b>    | Number of transitions from <b>Down</b> to <b>Up</b> condition.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Status</b>        | Status of the (local or remote circuit) local interface: <ul style="list-style-type: none"> <li>• <b>Up</b>—Operational</li> <li>• <b>Dn</b>—Down</li> <li>• <b>NP</b>—Not present</li> <li>• <b>DS</b>—Disabled</li> <li>• <b>WE</b>—Wrong encapsulation</li> <li>• <b>UN</b>—Uninitialized</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Encapsulation</b> | Type of encapsulation: <b>VPLS</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Remote PE</b>     | Address of the remote provider edge router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

Table 35: show vpls connections Output Fields (*continued*)

| Field Name                      | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Negotiated control-word</b>  | Whether a control word has been negotiated: <b>Yes</b> or <b>No</b> .                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Incoming label</b>           | Name of the incoming label.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Outgoing label</b>           | Name of the outgoing label.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Negotiated PW status TLV</b> | Indicates whether or not the pseudowire status TLV has been negotiated for the VPLS connection.                                                                                                                                                                                                                                                                                                                                                              |
| <b>Local interface</b>          | Provides the following information about the local interface configured for the VPLS neighbor: <ul style="list-style-type: none"> <li>• Name of the local interface</li> <li>• <b>Status</b>—Interface status (<b>Up</b> or <b>Down</b>)</li> <li>• <b>Encapsulation</b>—Interface encapsulation (for example, <b>ETHERNET</b>)</li> <li>• <b>Description</b>—Includes the VPLS instance name, the VPLS neighbor address, and the VPLS identifier</li> </ul> |
| <b>Time</b>                     | Date and time of VPLS connection event.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Event</b>                    | Type of event.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Interface/Lbl/PE</b>         | Interface, label, or PE router.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Connection History</b>       | Each entry can include the date, time, year, and the connection event. Connection events include any of a variety of events related to VPLS connections, such as route changes, label updates, and interfaces going down or coming up.                                                                                                                                                                                                                       |

## Sample Output

### show vpls connections

```
user@host> show vpls connections
Layer-2 VPN connections:
```

#### Legend for connection status (St)

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| EI -- encapsulation invalid      | NC -- interface encapsulation not CCC/TCC/VPLS |
| EM -- encapsulation mismatch     | WE -- interface and instance encaps not same   |
| VC-Dn -- Virtual circuit down    | NP -- interface hardware not present           |
| CM -- control-word mismatch      | -< -- only outbound connection is up           |
| CN -- circuit not provisioned    | >- -- only inbound connection is up            |
| OR -- out of range               | Up -- operational                              |
| OL -- no outgoing label          | Dn -- down                                     |
| LD -- local site signaled down   | CF -- call admission control failure           |
| RD -- remote site signaled down  | SC -- local and remote site ID collision       |
| LN -- local site not designated  | LM -- local site ID not minimum designated     |
| RN -- remote site not designated | RM -- remote site ID not minimum designated    |
| XX -- unn connection status      | IL -- no incoming label                        |
| MM -- MTU mismatch               | MI -- Mesh-Group ID not availble               |
| BK -- Backup connection          | ST -- Standby connection                       |

PF -- Profile parse failure      PB -- Profile busy

Legend for interface status  
Up -- operational  
Dn -- down

Instance: vpls-1  
Local site: 1 (11)  
Number of local interfaces: 1  
Number of local interfaces up: 1  
IRB interface present: no  
lt-1/3/0.10496

|                  |   |                                                |
|------------------|---|------------------------------------------------|
| vt-1/3/0.1048588 | 1 | Intf - vpls vpls-1 local site 11 remote site 1 |
| vt-1/2/0.1048591 | 2 | Intf - vpls vpls-1 local site 11 remote site 2 |
| vt-1/2/0.1048585 | 3 | Intf - vpls vpls-1 local site 11 remote site 3 |
| vt-1/2/0.1048587 | 4 | Intf - vpls vpls-1 local site 11 remote site 4 |
| vt-1/2/0.1048589 | 5 | Intf - vpls vpls-1 local site 11 remote site 5 |
| vt-1/3/0.1048586 | 6 | Intf - vpls vpls-1 local site 11 remote site 6 |
| vt-1/3/0.1048590 | 7 | Intf - vpls vpls-1 local site 11 remote site 7 |
| vt-1/3/0.1048584 | 8 | Intf - vpls vpls-1 local site 11 remote site 8 |

|            |        |      |       |            |
|------------|--------|------|-------|------------|
| Label-base | Offset | Size | Range | Preference |
| + 800256   | 1      | 16   | 16    | 100        |

Timer Values:  
Startup wait time: 120 seconds  
New site wait-time: 20 seconds  
Collision detect time: 30 seconds  
Reclaim wait time: 748 milliseconds

|                 |      |    |                      |            |
|-----------------|------|----|----------------------|------------|
| connection-site | Type | St | Time last up         | # Up trans |
| 1               | rmt  | Up | Apr 28 13:28:24 2009 | 2          |

Remote PE: 192.0.2.1, Negotiated control-word: No  
Incoming label: 800256, Outgoing label: 800026  
Local interface: vt-1/3/0.1048588, Status: Up, Encapsulation: VPLS  
Description: Intf - vpls vpls-1 local site 11 remote site 1

Connection History:

|                      |                              |
|----------------------|------------------------------|
| Apr 28 13:28:24 2009 | status update timer          |
| Apr 28 13:28:24 2009 | PE route down                |
| Apr 28 13:24:27 2009 | status update timer          |
| Apr 28 13:24:27 2009 | loc intf up vt-1/3/0.1048588 |
| Apr 28 13:24:27 2009 | PE route changed             |
| Apr 28 13:24:27 2009 | Out lbl Update 800026        |
| Apr 28 13:24:27 2009 | In lbl Update 800256         |
| Apr 28 13:24:27 2009 | loc intf down                |

|   |     |    |                      |   |
|---|-----|----|----------------------|---|
| 2 | rmt | Up | Apr 28 13:28:24 2009 | 2 |
|---|-----|----|----------------------|---|

Remote PE: 192.0.2.7, Negotiated control-word: No  
Incoming label: 800257, Outgoing label: 800034  
Local interface: vt-1/2/0.1048591, Status: Up, Encapsulation: VPLS  
Description: Intf - vpls vpls-1 local site 11 remote site 2

Connection History:

|                      |                              |
|----------------------|------------------------------|
| Apr 28 13:28:24 2009 | status update timer          |
| Apr 28 13:28:24 2009 | PE route down                |
| Apr 28 13:24:28 2009 | status update timer          |
| Apr 28 13:24:28 2009 | loc intf up vt-1/2/0.1048591 |
| Apr 28 13:24:28 2009 | PE route changed             |

```

Apr 28 13:24:28 2009 Out lbl Update 800034
Apr 28 13:24:28 2009 In lbl Update 800257
Apr 28 13:24:28 2009 loc intf down
3 rmt Up Apr 28 13:28:24 2009 2
Remote PE: 192.0.2.14, Negotiated control-word: No
Incoming label: 800258, Outgoing label: 800026
Local interface: vt-1/2/0.1048585, Status: Up, Encapsulation: VPLS
Description: Intf - vpls vpls-1 local site 11 remote site 3
Connection History:
Apr 28 13:28:24 2009 status update timer
Apr 28 13:28:24 2009 PE route down
Apr 28 13:24:26 2009 status update timer
Apr 28 13:24:26 2009 loc intf up vt-1/2/0.1048585
Apr 28 13:24:26 2009 PE route changed
Apr 28 13:24:26 2009 Out lbl Update 800026
Apr 28 13:24:26 2009 In lbl Update 800258
Apr 28 13:24:26 2009 loc intf down
4 rmt Up Apr 28 13:28:24 2009 2
Remote PE: 192.0.2.16, Negotiated control-word: No
Incoming label: 800259, Outgoing label: 800026
Local interface: vt-1/2/0.1048587, Status: Up, Encapsulation: VPLS
Description: Intf - vpls vpls-1 local site 11 remote site 4
Connection History:
Apr 28 13:28:24 2009 status update timer
Apr 28 13:28:24 2009 PE route down
Apr 28 13:24:27 2009 status update timer
Apr 28 13:24:27 2009 loc intf up vt-1/2/0.1048587
Apr 28 13:24:27 2009 PE route changed
Apr 28 13:24:27 2009 Out lbl Update 800026
Apr 28 13:24:27 2009 In lbl Update 800259
Apr 28 13:24:27 2009 loc intf down
5 rmt Up Apr 28 13:28:24 2009 2
Remote PE: 192.0.2.13, Negotiated control-word: No
Incoming label: 800260, Outgoing label: 800034
Local interface: vt-1/2/0.1048589, Status: Up, Encapsulation: VPLS
Description: Intf - vpls vpls-1 local site 11 remote site 5
Connection History:
Apr 28 13:28:24 2009 status update timer
Apr 28 13:28:24 2009 PE route down
Apr 28 13:24:28 2009 status update timer
Apr 28 13:24:28 2009 loc intf up vt-1/2/0.1048589
Apr 28 13:24:28 2009 PE route changed
Apr 28 13:24:28 2009 Out lbl Update 800034
Apr 28 13:24:27 2009 In lbl Update 800260
Apr 28 13:24:27 2009 loc intf down

```

### show vpls connections (with multiple pseudowires)

```

user@host> show vpls connections
Layer-2 VPN connections:

```

#### Legend for connection status (St)

```

EI -- encapsulation invalid NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down NP -- interface hardware not present
CM -- control-word mismatch -> -- only outbound connection is up
CN -- circuit not provisioned <- -- only inbound connection is up
OR -- out of range Up -- operational
OL -- no outgoing label Dn -- down
LD -- local site signaled down CF -- call admission control failure
RD -- remote site signaled down SC -- local and remote site ID collision

```

```

LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status IL -- no incoming label
MM -- MTU mismatch MI -- Mesh-Group ID not available
BK -- Backup connection ST -- Standby connection
PF -- Profile parse failure PB -- Profile busy
RS -- remote site standby SN -- Static Neighbor
LB -- Local site not best-site RB -- Remote site not best-site
VM -- VLAN ID mismatch

```

#### Legend for interface status

```

Up -- operational
Dn -- down

```

Instance: vpls

VPLS-id: 100

Mesh-group connections: \_\_ves\_\_

```

Neighbor Type St Time last up # Up trans
10.255.114.3 (vpls-id 100) rmt Up Apr 11 23:38:38 2013 1
Remote PE: 10.255.114.3, Negotiated control-word: No
Incoming label: 262145, Outgoing label: 262145
Negotiated PW status TLV: No
Local interface: lsi.1049090, Status: Up, Encapsulation: ETHERNET
Description: Intf - vpls h-vpls neighbor 10.255.114.3 vpls-id 100

```

Mesh-group connections: spokes

```

Neighbor Type St Time last up # Up trans
10.255.114.4 (vpls-id 200) rmt Up Apr 11 23:39:25 2013 1
Remote PE: 10.255.114.4, Negotiated control-word: No
Incoming label: 262148, Outgoing label: 304224
Negotiated PW status TLV: Yes
Local PW status code: 0x00000000, Neighbor PW status code: 0x00000000
Local interface: lsi.1049091, Status: Up, Encapsulation: ETHERNET
Description: Intf - vpls h-vpls neighbor 10.255.114.4 vpls-id 200
10.255.114.4 (vpls-id 201) rmt Up Apr 11 23:39:25 2013 1
Remote PE: 10.255.114.4, Negotiated control-word: No
Incoming label: 262149, Outgoing label: 304225
Negotiated PW status TLV: Yes
Local PW status code: 0x00000000, Neighbor PW status code: 0x00000000
Local interface: lsi.1049096, Status: Up, Encapsulation: ETHERNET
Description: Intf - vpls h-vpls neighbor 10.255.114.4 vpls-id 201

```

#### show vpls connections extensive (Static VPLS Neighbors)

```
user@host> show vpls connections extensive instance red
```

Layer-2 VPN connections:

#### Legend for connection status (St)

```

EI -- encapsulation invalid NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down NP -- interface hardware not present
CM -- control-word mismatch -> -- only outbound connection is up
CN -- circuit not provisioned <- -- only inbound connection is up
OR -- out of range Up -- operational
OL -- no outgoing label Dn -- down
LD -- local site signaled down CF -- call admission control failure
RD -- remote site signaled down SC -- local and remote site ID collision
LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status IL -- no incoming label
MM -- MTU mismatch MI -- Mesh-Group ID not available

```

```

BK -- Backup connection ST -- Standby connection
PF -- Profile parse failure PB -- Profile busy
RS -- remote site standby SN -- Static Neighbor

Legend for interface status
Up -- operational
Dn -- down

Instance: static
VPLS-id: 1
Number of local interfaces: 1
Number of local interfaces up: 1
ge-0/0/5.0
lsi.1049344 Intf - vpls static neighbor 10.255.114.3 vpls-id
1
Neighbor Type St Time last up # Up trans
10.255.114.3(vpls-id 1)(SN) rmt Up Mar 4 08:48:41 2010 1
Remote PE: 10.255.114.3, Negotiated control-word: No
Incoming label: 29696, Outgoing label: 29697
Negotiated PW status TLV: No
Local interface: lsi.1049344, Status: Up, Encapsulation: ETHERNET
Description: Intf - vpls static neighbor 10.255.114.3 vpls-id 1
Connection History:
Mar 4 08:48:41 2010 status update timer
Mar 4 08:48:41 2010 PE route changed
Mar 4 08:48:41 2010 Out lbl Update 29697
Mar 4 08:48:41 2010 In lbl Update 29696
Mar 4 08:48:41 2010 loc intf up lsi.1049344

user@PE1> show vpls connections extensive (Multihoming with FEC 129)
Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down NP -- interface hardware not present
CM -- control-word mismatch -> -- only outbound connection is up
CN -- circuit not provisioned <- -- only inbound connection is up
OR -- out of range Up -- operational
OL -- no outgoing label Dn -- down
LD -- local site signaled down CF -- call admission control failure
RD -- remote site signaled down SC -- local and remote site ID collision
LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status IL -- no incoming label
MM -- MTU mismatch MI -- Mesh-Group ID not available
BK -- Backup connection ST -- Standby connection
PF -- Profile parse failure PB -- Profile busy
RS -- remote site standby SN -- Static Neighbor
LB -- Local site not best-site RB -- Remote site not best-site
VM -- VLAN ID mismatch

Legend for interface status
Up -- operational
Dn -- down

Instance: green
L2vpn-id: 100:100
Local-id: 192.0.2.2
Number of local interfaces: 2
Number of local interfaces up: 2

```

```

ge-0/3/1.0
ge-0/3/3.0
lsi.101711873 Intf - vpls green local-id 192.0.2.2 remote-id
192.0.2.4 neighbor 192.0.2.4
 Remote-id Type St Time last up # Up trans
 192.0.2.4 rmt Up Jan 31 13:49:52 2012 1
 Remote PE: 192.0.2.4, Negotiated control-word: No
 Incoming label: 262146, Outgoing label: 262146
 Local interface: lsi.101711873, Status: Up, Encapsulation: ETHERNET
 Description: Intf - vpls green local-id 192.0.2.2 remote-id 192.0.2.4
neighbor 192.0.2.4
 Connection History:
 Jan 31 13:49:52 2012 status update timer
 Jan 31 13:49:52 2012 PE route changed
 Jan 31 13:49:52 2012 Out lbl Update 262146
 Jan 31 13:49:52 2012 In lbl Update 262146
 Jan 31 13:49:52 2012 loc intf up lsi.101711873
Multi-home:
 Local-site Id Pref State
 test 1 100 Up
 Number of interfaces: 1
 Number of interfaces up: 1
 ge-0/3/1.0
 Received multi-homing advertisements:
 Remote-PE Pref flag Description
 192.0.2.4 100 0x0

```

## show vpls flood event-queue

|                                 |                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show vpls flood event-queue                                                                                                                                                               |
| <b>Release Information</b>      | Command introduced in Junos OS Release 8.0.                                                                                                                                               |
| <b>Description</b>              | Display the pending events in the VPLS flood queue.                                                                                                                                       |
| <b>Options</b>                  | This command has no options.                                                                                                                                                              |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                      |
| <b>List of Sample Output</b>    | <a href="#">show vpls flood event-queue on page 1316</a>                                                                                                                                  |
| <b>Output Fields</b>            | <a href="#">Table 36 on page 1316</a> lists the output fields for the <b>show vpls flood event-queue</b> command. Output fields are listed in the approximate order in which they appear. |

**Table 36: show vpls flood event-queue Output Fields**

| Field Name                   | Field Description                                                        |
|------------------------------|--------------------------------------------------------------------------|
| <b>Current Pending Event</b> | Provides information on the current event in the VPLS flood event queue. |
| <b>Name</b>                  | Name of the event.                                                       |
| <b>Owner Name</b>            | Name of the interface associated with the flood event.                   |
| <b>Pending Op</b>            | Pending operation for the event.                                         |
| <b>Last Error</b>            | Name of the last error encountered.                                      |
| <b>Number of Retries</b>     | Number of attempts made to update the event queue.                       |
| <b>Pending Event List</b>    | List of the events awaiting processing.                                  |
| <b>Event Name</b>            | Name of the event.                                                       |
| <b>Pending Op</b>            | Pending operation for the event.                                         |
| <b>Event Identifier</b>      | Name of the interface associated with the flood event.                   |

## Sample Output

### show vpls flood event-queue

```

user@host> show vpls flood event-queue
Current Pending Event
 Name: Flood Nexthop
 Owner Name: ge-4/3/0.0
 Pending Op: ADD

```



```
Last Error:ENOMEM
Number of Retries:3
Pending Event List:
Event Name Pending Op Event Identifier
Flood Nexthop ADD ge-4/3/0.0
Flood Route ADD ge-4/3/0.0
```

## show vpls flood instance

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show vpls flood instance<br><brief   detail   extensive><br><instance-name><br><logical-system <i>logical-system-name</i> >                                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Command introduced in Junos OS Release 8.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Display VPLS information related to the flood process.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Options</b>                  | <p><b>none</b>—Display VPLS information related to the flood process for all routing instances.</p> <p><b>brief   detail   extensive</b>—(Optional) Display the specified level of output.</p> <p><b>instance-name</b>—(Optional) Display VPLS information related to the flood process for the specified routing instance.</p> <p><b>logical-system <i>logical-system-name</i></b>—(Optional) Display VPLS information related to the flood process for the specified logical system.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>List of Sample Output</b>    | <a href="#">show vpls flood instance on page 1319</a><br><a href="#">show vpls flood instance logical-system-name on page 1319</a><br><a href="#">show vpls flood instance detail on page 1319</a>                                                                                                                                                                                                                                                                                         |
| <b>Output Fields</b>            | Table 37 on page 1318 lists the output fields for the <b>show vpls flood instance</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                     |

**Table 37: show vpls flood instance Output Fields**

| Field Name            | Field Description                                             |
|-----------------------|---------------------------------------------------------------|
| <b>Logical system</b> | Name of the logical system.                                   |
| <b>Name</b>           | Name of the VPLS routing instance.                            |
| <b>CEs</b>            | Number of CE routers connected to the VPLS instance.          |
| <b>VEs</b>            | Number of VE routers connected to the VPLS instance.          |
| <b>Flood routes</b>   | List of all flood routes associated with the VPLS instance.   |
| <b>Prefix</b>         | Prefix for the route.                                         |
| <b>Type</b>           | Type of route.                                                |
| <b>Owner</b>          | VPLS routing instance or interface associated with the route. |
| <b>Nhype</b>          | Next-hop type. For example, <b>flood</b> for a flood route.   |

Table 37: show vpls flood instance Output Fields (*continued*)

| Field Name | Field Description                    |
|------------|--------------------------------------|
| Nhindex    | Next-hop index number for the route. |

## Sample Output

### show vpls flood instance

```
user@host> show vpls flood instance

Logical system: __juniper_ls1__
Name: green
CEs: 1
VEs: 1
Flood Routes:
 Prefix Type Owner NhType NhIndex
 default ALL_CE_FLOOD green flood 383
 0x47/16 CE_FLOOD fe-1/2/1.0 flood 388
```

### show vpls flood instance logical-system-name

```
user@host: __juniper_ls1__> show vpls flood instance juniper_ls1

Logical system: __juniper_ls1__
Name: green
CEs: 1
VEs: 1
Flood Routes:
 Prefix Type Owner NhType NhIndex
 default ALL_CE_FLOOD green flood 383
 0x47/16 CE_FLOOD fe-1/2/1.0 flood 388
```

### show vpls flood instance detail

```
user@host: __juniper_ls1__> show vpls flood instance detail

Logical system: __juniper_ls1__
Name: green
CEs: 1
VEs: 1
Flood Routes:
 Prefix Type Owner NhType NhIndex
 default ALL_CE_FLOOD green flood 383
 0x47/16 CE_FLOOD fe-1/2/1.0 flood 388
```

## show vpls flood route

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show vpls flood route<br>(all-ce-flood instance-name <i>instance-name</i> <logical-system-name <i>logical-system-name</i> ><br> <br>ce-flood interface <i>interface-name</i> )                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Command introduced in Junos OS Release 8.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | Display VPLS route information related to the flood process for either the specified routing instance or the specified interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Options</b>                  | <p><b>all-ce-flood</b>—Display the flood next-hop route for all customer edge routers for traffic coming from the core of the network.</p> <p><b>ce-flood interface <i>interface-name</i></b>—Display the flood next-hop route for traffic coming from the specified customer edge interface.</p> <p><b>instance-name <i>instance-name</i></b>—Display the flood routes for the specified instance.</p> <p><b>logical-system-name <i>logical-system-name</i></b>—(Optional) Specify the logical system whose flood routes you want to display. You can only specify the default logical system name for VPLS. The default logical system name is <b>__juniper_ls1__</b> (the name must be entered in the command with the underscore characters).</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>List of Sample Output</b>    | <a href="#">show vpls flood route all-ce-flood on page 1321</a><br><a href="#">show vpls flood route ce-flood on page 1321</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Output Fields</b>            | <a href="#">Table 38 on page 1320</a> lists the output for the <b>show vpls flood route</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

**Table 38: show vpls flood route Output Fields**

| Field Name             | Field Description                                                     |
|------------------------|-----------------------------------------------------------------------|
| Flood route prefix     | Prefix for the flood route.                                           |
| Flood route type       | Type of flood route (either <b>CE_FLOOD</b> or <b>ALL_CE_FLOOD</b> ). |
| Flood route owner      | VPLS routing instance or interface associated with the flood route.   |
| Nexthop type           | Next-hop type. For example, <b>flood</b> for a flood route.           |
| Nexthop index          | Next-hop index number for the route.                                  |
| Interfaces flooding to | Interfaces to which VPLS routes are being flooded.                    |
| Name                   | Name of the interface.                                                |

Table 38: show vpls flood route Output Fields (*continued*)

| Field Name | Field Description                 |
|------------|-----------------------------------|
| Type       | Type of VPLS router (CE or VE).   |
| Nh type    | Next-hop type.                    |
| Index      | Index number for the flood route. |

## Sample Output

### show vpls flood route all-ce-flood

```
user@host:~juniper_ls1~> show vpls flood route all-ce-flood logical-system-name
~juniper_ls1_instance-name green
```

```
Flood route prefix: default
Flood route type: ALL_CE_FLOOD
Flood route owner: green
Nexthop type: flood
Nexthop index: 383
 Interfaces Flooding to:
 Name Type NhType Index
 fe-1/2/1.0 CE
```

### show vpls flood route ce-flood

```
user@host:~juniper_ls1~> show vpls flood route ce-flood interface fe-1/2/1.0
```

```
Flood route prefix: 0x47/16
Flood route type: CE_FLOOD
Flood route owner: fe-1/2/1.0
Nexthop type: flood
Nexthop index: 388
 Interfaces Flooding to:
 Name Type NhType Index
 lsi.49152 VE indr 262142
```

## show vpls mac-move-action

|                                 |                                                                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show vpls mac-move-action instance</b><br><b>&lt;instance <i>instance-name</i>&gt;</b>                                                                                            |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.2.                                                                                                                                         |
| <b>Description</b>              | Display the learning interfaces (IFLs) disabled due to a MAC move in a VPLS instance.                                                                                                |
| <b>Options</b>                  | <b>none</b> —Display all the IFLs disabled due to MAC moves.<br><br><b>instance <i>instance-name</i></b> —(Optional) Display the IFLs disabled due to a MAC move in a VPLS instance. |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                 |
| <b>List of Sample Output</b>    | <a href="#">show vpls mac-move-action (MX Series) on page 1322</a><br><a href="#">show vpls mac-move-action instance instance-name on page 1323</a>                                  |
| <b>Output Fields</b>            | Table 39 on page 1322 describes the output fields for the <b>show vpls mac-move-action</b> command. Output fields are listed in the approximate order in which they appear.          |

Table 39: show vpls mac-move-action Output Fields

| Field Name      | Field Description                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Instance        | Instance name                                                                                                                                                      |
| Local Interface | Local interface disabled due to MAC move.                                                                                                                          |
| Index           | Index number.                                                                                                                                                      |
| Algorithm Used  | The following algorithm can be in use: <ul style="list-style-type: none"> <li>• Base IFL — Primary approach</li> <li>• Statistical — Secondary approach</li> </ul> |
| Time rec        | Time recorded in hh:mm:sec.                                                                                                                                        |
| Recovery Timer  | Enable the interface after a set time.                                                                                                                             |

## Sample Output

### show vpls mac-move-action (MX Series)

```

user@host> show vpls mac-move-action

Instance: vpls_1
Local interface: xe-1/3/1.600, Index: 341
Algorithm used : Statistical
Time rec : 02:30:35
Recovery timer : Yes

```

**show vpls mac-move-action instance instance-name**

```
user@host> show vpls mac-move-action instance vpls_1
```

```
Instance: vpls_1
Local interface: xe-1/3/1.600, Index: 341
Algorithm used : Base IFL
Time rec : 02:29:35
Recovery timer : Yes
```

## show vpls mac-table

---

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                   | <b>show vpls mac-table</b><br><brief   detail   extensive   summary><br><bridge-domain <i>bridge-domain-name</i> ><br><instance <i>instance-name</i> ><br><interface <i>interface-name</i> ><br><logical-system (all   <i>logical-system-name</i> )><br><mac-address><br><vlan-id <i>vlan-id-number</i> >                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Release Information      | Command introduced in Junos OS Release 8.5.<br>Command introduced in Junos OS Release 15.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Description              | Display learned virtual private LAN service (VPLS) media access control (MAC) address information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Options                  | <b>none</b> —Display all learned VPLS MAC address information.<br><br><b>brief   detail   extensive   summary</b> —(Optional) Display the specified level of output.<br><br><b>bridge-domain <i>bridge-domain-name</i></b> —(Optional) Display learned VPLS MAC addresses for the specified bridge domain.<br><br><b>instance <i>instance-name</i></b> —(Optional) Display learned VPLS MAC addresses for the specified instance.<br><br><b>interface <i>interface-name</i></b> —(Optional) Display learned VPLS MAC addresses for the specified instance.<br><br><b>logical-system (all   <i>logical-system-name</i>)</b> —(Optional) Display learned VPLS MAC addresses for all logical systems or for the specified logical system.<br><br><b>mac-address</b> —(Optional) Display the specified learned VPLS MAC address information..<br><br><b>vlan-id <i>vlan-id-number</i></b> —(Optional) Display learned VPLS MAC addresses for the specified VLAN. |
| Required Privilege Level | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| List of Sample Output    | <a href="#">show vpls mac-table on page 1325</a><br><a href="#">show vpls mac-table (with Layer 2 Services over GRE Interfaces) on page 1326</a><br><a href="#">show vpls mac-table (with VXLAN enabled) on page 1326</a><br><a href="#">show vpls mac-table count on page 1326</a><br><a href="#">show vpls mac-table detail on page 1327</a><br><a href="#">show vpls mac-table extensive on page 1327</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Output Fields            | <a href="#">Table 40 on page 1325</a> describes the output fields for the <b>show vpls mac-table</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |



Table 40: show vpls mac-table Output fields

| Field Name              | Field Description                                                                                                                                                                                                                                                                                  |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Routing instance        | Name of the routing instance.                                                                                                                                                                                                                                                                      |
| Bridging domain         | Name of the bridging domain.                                                                                                                                                                                                                                                                       |
| MAC address             | MAC address or addresses learned on a logical interface.                                                                                                                                                                                                                                           |
| MAC flags               | Status of MAC address learning properties for each interface: <ul style="list-style-type: none"> <li>• <b>S</b>—Static MAC address configured.</li> <li>• <b>D</b>—Dynamic MAC address learned.</li> <li>• <b>SE</b>—MAC accounting is enabled.</li> <li>• <b>NM</b>—Nonconfigured MAC.</li> </ul> |
| Logical interface       | Name of the logical interface.                                                                                                                                                                                                                                                                     |
| MAC count               | Number of MAC addresses learned on a specific routing instance or interface.                                                                                                                                                                                                                       |
| Learning interface      | Logical interface or logical Label Switched Interface (LSI) the address is learned on.                                                                                                                                                                                                             |
| Base learning interface | Base learning interface of the MAC address. This field is introduced in Junos OS Release 14.2.                                                                                                                                                                                                     |
| Learn VLAN ID/VLAN      | VLAN ID of the routing instance or bridge domain in which the MAC address was learned.                                                                                                                                                                                                             |
| VXLAN ID/VXLAN          | VXLAN Network Identifier (VNI)                                                                                                                                                                                                                                                                     |
| Layer 2 flags           | Debugging flags signifying that the MAC address is present in various lists.                                                                                                                                                                                                                       |
| Epoch                   | Spanning Tree Protocol epoch number identifying when the MAC address was learned. Used for debugging.                                                                                                                                                                                              |
| Sequence number         | Sequence number assigned to this MAC address. Used for debugging.                                                                                                                                                                                                                                  |
| Learning mask           | Mask of Packet Forwarding Engines where this MAC address was learned. Used for debugging.                                                                                                                                                                                                          |
| IPC generation          | Creation time of the logical interface when this MAC address was learned. Used for debugging.                                                                                                                                                                                                      |

## Sample Output

### show vpls mac-table

```

user@host> show vpls mac-table
MAC flags (S -static MAC, D -dynamic MAC,
 SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vpls_ldp1
VLAN : 223
 MAC MAC Logical
 address flags interface
 00:90:69:9c:1c:5d D ge-0/2/5.400

```

MAC flags (S -static MAC, D -dynamic MAC,  
SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vpls\_red  
VLAN : 401

| MAC<br>address    | MAC<br>flags | Logical<br>interface |
|-------------------|--------------|----------------------|
| 00:00:aa:12:12:12 | D            | lsi.1051138          |
| 00:05:85:74:9f:f0 | D            | lsi.1051138          |

#### show vpls mac-table (with Layer 2 Services over GRE Interfaces)

user@host> show vpls mac-table  
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned  
SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : vpls\_4site:1000  
Bridging domain : \_\_vpls\_4site:1000\_\_, MAC

| MAC<br>address    | MAC<br>flags | Logical<br>interface |
|-------------------|--------------|----------------------|
| 00:01:01:00:01:f4 | D,SE         | ge-4/2/0.1000        |
| 00:02:01:33:01:f4 | D,SE         | lsi.1052004          |
| 00:03:00:32:01:f4 | D,SE         | lsi.1048840          |
| 00:04:00:14:01:f4 | D,SE         | lsi.1052005          |
| 00:02:01:33:02:f7 | D,SE         | gr-1/2/10.10         |

#### show vpls mac-table (with VXLAN enabled)

user@host> show vpls mac-table  
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned  
SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : vpls\_4site:1000  
Bridging domain : \_\_vpls\_4site:1000\_\_, VLAN : 4094,4093  
VXLAN: Id : 300, Multicast group: 226.1.1.3

| MAC<br>address    | MAC<br>flags | Logical<br>interface |
|-------------------|--------------|----------------------|
| 00:01:01:00:01:f4 | D,SE         | ge-4/2/0.1000        |
| 00:02:01:33:01:f4 | D,SE         | lsi.1052004          |
| 00:03:00:32:01:f4 | D,SE         | lsi.1048840          |
| 00:04:00:14:01:f4 | D,SE         | lsi.1052005          |
| 00:02:01:33:02:f7 | D,SE         | vtep.1052010         |
| 00:04:00:14:02:f7 | D,SE         | vtep.1052011         |

#### show vpls mac-table count

user@host> show vpls mac-table count  
0 MAC address learned in routing instance \_\_juniper\_private1\_\_

MAC address count per interface within routing instance:

| Logical interface | MAC count |
|-------------------|-----------|
| lc-0/0/0.32769    | 0         |
| lc-0/1/0.32769    | 0         |
| lc-0/2/0.32769    | 0         |
| lc-2/0/0.32769    | 0         |
| lc-0/3/0.32769    | 0         |
| lc-2/1/0.32769    | 0         |
| lc-9/0/0.32769    | 0         |
| lc-11/0/0.32769   | 0         |
| lc-2/2/0.32769    | 0         |
| lc-9/1/0.32769    | 0         |
| lc-11/1/0.32769   | 0         |

|                 |   |
|-----------------|---|
| 1c-2/3/0.32769  | 0 |
| 1c-9/2/0.32769  | 0 |
| 1c-11/2/0.32769 | 0 |
| 1c-11/3/0.32769 | 0 |
| 1c-9/3/0.32769  | 0 |

MAC address count per learn VLAN within routing instance:

| Learn VLAN ID | MAC count |
|---------------|-----------|
| 0             | 0         |

1 MAC address learned in routing instance vpls\_ldp1

MAC address count per interface within routing instance:

| Logical interface | MAC count |
|-------------------|-----------|
| lsi.1051137       | 0         |
| ge-0/2/5.400      | 1         |

MAC address count per learn VLAN within routing instance:

| Learn VLAN ID | MAC count |
|---------------|-----------|
| 0             | 1         |

1 MAC address learned in routing instance vpls\_red

MAC address count per interface within routing instance:

| Logical interface | MAC count |
|-------------------|-----------|
| ge-0/2/5.300      | 1         |

MAC address count per learn VLAN within routing instance:

| Learn VLAN ID | MAC count |
|---------------|-----------|
| 0             | 1         |

### show vpls mac-table detail

```

user@host> show vpls mac-table detail
MAC address: 00:90:69:9c:1c:5d
Routing instance: vpls_ldp1
Learning interface: ge-0/2/5.400
Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
Epoch: 0 Sequence number: 1
Learning mask: 0x1 IPC generation: 0

MAC address: 00:90:69:9c:1c:5d
Routing instance: vpls_red
Learning interface: ge-0/2/5.300
Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
Epoch: 0 Sequence number: 1
Learning mask: 0x1 IPC generation: 0

```

### show vpls mac-table extensive

```

user@host> show vpls mac-table extensive

MAC address: 00:10:00:01:00:00
Routing instance: vpls_1
Bridging domain: __vpls_1__, VLAN : NA
Learning interface: lsi.1049165
Base learning interface: lsi.1049165
Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
Epoch: 0 Sequence number: 1
Learning mask: 0x00000001

```

```
MAC address: 00:10:00:01:00:01
Routing instance: vpls_1
 Bridging domain: __vpls_1__, VLAN : NA
 Learning interface: lsi.1049165
 Base learning interface: lsi.1049165
 Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
 Epoch: 0 Sequence number: 1
 Learning mask: 0x00000001

MAC address: 00:10:00:01:00:02
Routing instance: vpls_1
 Bridging domain: __vpls_1__, VLAN : NA
 Learning interface: lsi.1049165
 Base learning interface: lsi.1049165
 Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
 Epoch: 0 Sequence number: 1
 Learning mask: 0x00000001

MAC address: 00:10:00:01:00:03
Routing instance: vpls_1
 Bridging domain: __vpls_1__, VLAN : NA
 Learning interface: lsi.1049165
 Base learning interface: lsi.1049165
 Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
 Epoch: 0 Sequence number: 1
 Learning mask: 0x00000001
```

## show vpls statistics

|                                 |                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show vpls statistics<br><instance <i>instance-name</i> ><br><logical-system (all   <i>logical-system-name</i> )>                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | (T Series and M Series routers, except for the M160 router) Display virtual private LAN service (VPLS) statistics.                                                                                                                                                                                                                                          |
| <b>Options</b>                  | <p><b>none</b>—Display VPLS statistics for all routing instances.</p> <p><b>instance <i>instance-name</i></b>—(Optional) Display VPLS statistics for a specific VPLS routing instance only.</p> <p><b>logical-system (all   <i>logical-system-name</i>)</b>—(Optional) Perform this operation on all logical systems or on a particular logical system.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                        |
| <b>List of Sample Output</b>    | <a href="#">show vpls statistics on page 1330</a><br><a href="#">show vpls statistics instance on page 1330</a>                                                                                                                                                                                                                                             |
| <b>Output Fields</b>            | <a href="#">Table 41 on page 1329</a> lists the output fields for the <b>show vpls statistics</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                          |

**Table 41: show vpls statistics Output Fields**

| Field Name                         | Field Description                                                                                                                                                                                                                                   |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Instance</b>                    | Name of the VPLS instance.                                                                                                                                                                                                                          |
| <b>Local interface</b>             | Name of the local VPLS virtual loopback tunnel interface, <i>vt-fpc/plc/port.nnnnn</i> , where <i>nnnnn</i> is a dynamically generated virtual port used to transport and receive packets from other provider edge (PE) routers in the VPLS domain. |
| <b>Index</b>                       | Number associated with the next hop.                                                                                                                                                                                                                |
| <b>Remote provider edge router</b> | Address of the remote provider edge router.                                                                                                                                                                                                         |
| <b>Multicast packets</b>           | Number of multicast packets received.                                                                                                                                                                                                               |
| <b>Multicast bytes</b>             | Number of multicast bytes received.                                                                                                                                                                                                                 |
| <b>Flood packets</b>               | Number of VPLS flood packets received.                                                                                                                                                                                                              |
| <b>Flood bytes</b>                 | Number of VPLS flood bytes received.                                                                                                                                                                                                                |

Table 41: show vpls statistics Output Fields (*continued*)

| Field Name        | Field Description                                                                                                                     |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Current MAC count | Number of MAC addresses learned by the interface and the configured maximum limit on the number of MAC addresses that can be learned. |

## Sample Output

### show vpls statistics

```

user@host> show vpls statistics

VPLS statistics:

Instance: green

 Local interface: fe-2/2/1.0, Index: 69
 Multicast packets: 1
 Multicast bytes : 60
 Flooded packets : 18
 Flooded bytes : 2556
 Current MAC count: 1

 Local interface: lt-0/3/0.2, Index: 72
 Multicast packets: 3
 Multicast bytes : 153
 Flooded packets : 1
 Flooded bytes : 51
 Current MAC count: 1

 Local interface: lsi.32769, Index: 75
 Current MAC count: 0

 Local interface: lsi.32771, Index: 77
 Remote PE: 10.255.14.222
 Current MAC count: 2

Instance: red

 Local interface: vt-0/3/0.32768, Index: 74
 Multicast packets: 0
 Multicast bytes : 0
 Flooded packets : 0
 Flooded bytes : 0
 Current MAC count: 0

 Local interface: vt-0/3/0.32770, Index: 76
 Multicast packets: 0
 Multicast bytes : 0
 Flooded packets : 0
 Flooded bytes : 0
 Current MAC count: 0

```

### show vpls statistics instance

```

user@host> show vpls statistics instance red

```

## Layer-2 VPN Statistics:

Instance: red

Local interface: vt-3/2/0.32768, Index: 73

Remote provider edge router: 10.255.17.35

Multicast packets: 0

Multicast bytes : 0

Flood packets : 0

Flood bytes : 0

Current MAC count: 1 (Limit 20)





## PART 10

# Index

- [Index on page 1335](#)



# Index

## Symbols

|                                              |      |
|----------------------------------------------|------|
| #, comments in configuration statements..... | xxx  |
| ( ), in syntax descriptions.....             | xxx  |
| 802.1Q VLANs                                 |      |
| VLAN tagging.....                            | 1226 |
| < >, in syntax descriptions.....             | xxx  |
| [ ], in configuration statements.....        | xxx  |
| { }, in configuration statements.....        | xxx  |
| (pipe), in syntax descriptions.....          | xxx  |

## A

|                                       |          |
|---------------------------------------|----------|
| action-priority statement.....        | 1069     |
| Active role.....                      | 452, 490 |
| active routes.....                    | 169      |
| active-interface statement.....       | 1070     |
| usage guidelines.....                 | 754      |
| Active-Standby.....                   | 249      |
| Active-Standby Multihoming            |          |
| extended community.....               | 249      |
| implementation.....                   | 249      |
| NLRI.....                             | 249      |
| route type.....                       | 249      |
| sample configuration.....             | 249      |
| traffic flow                          |          |
| BUM.....                              | 249      |
| unicast.....                          | 249      |
| updates to forwarding table           |          |
| MAC.....                              | 249      |
| MPLS.....                             | 249      |
| address prefix, source or destination |          |
| firewall filter match conditions      |          |
| VPLS traffic.....                     | 926      |
| address, source or destination        |          |
| firewall filter match conditions      |          |
| VPLS traffic.....                     | 926      |
| aggregate-label statement.....        | 1038     |
| usage guidelines.....                 | 21       |
| aggregated Ethernet interfaces        |          |
| VPLS, configuring.....                | 608      |
| VPLS, overview.....                   | 609      |
| All.....                              | 452, 489 |

|                                    |          |
|------------------------------------|----------|
| always-compare-med option.....     | 169      |
| any statement.....                 | 1071     |
| as-path-ignore                     |          |
| usage guidelines.....              | 169      |
| ATM trunking.....                  | 365      |
| Layer 2 circuits.....              | 361      |
| auto-discovery-only statement      |          |
| BGP.....                           | 1072     |
| autodiscovery statement            |          |
| BGP for LDP VPLS                   |          |
| usage guidelines.....              | 725, 742 |
| VPWS.....                          | 459, 713 |
| automatic route distinguisher..... | 14       |
| automatic-site-id statement.....   | 1073     |
| usage guidelines.....              | 566      |
| autonomous system number           |          |
| route distinguisher.....           | 13, 240  |

## B

|                                          |                    |
|------------------------------------------|--------------------|
| backup-interface.....                    | 1074               |
| backup-neighbor statement.....           | 1039               |
| usage guidelines.....                    | 180                |
| bandwidth accounting.....                | 363                |
| bandwidth statement.....                 | 1075               |
| Layer 2 circuits                         |                    |
| usage guidelines.....                    | 365                |
| Base IFL.....                            | 900, 901, 903, 904 |
| best-site statement.....                 | 1076               |
| BFD.....                                 | 433, 435           |
| VCCV.....                                | 188                |
| BFD for VCCV.....                        | 188                |
| Layer 2 VPNs Layer 2 circuits, VPLS..... | 188                |
| bfd-liveness-detection statement.....    | 1077               |
| BFD                                      |                    |
| threshold.....                           | 1207               |
| transmit-interval.....                   | 1218               |
| usage guidelines.....                    | 186                |
| BGP                                      |                    |
| BGP_L2VPN_AD_NLRI.....                   | 1072               |
| FEC 129.....                             | 1072               |
| LDP-based Layer 2 VPN and VPLS update    |                    |
| messages .....                           | 1072               |
| MP-BGP.....                              | 1105               |
| proxy route target filtering.....        | 50, 51, 1048, 1055 |
| route target filtering.....              | 38, 41             |
| export policy.....                       | 66                 |
| BGP and LDP signaling, VPLS.....         | 554                |

|                                                 |                          |
|-------------------------------------------------|--------------------------|
| BGP autodiscovery                               |                          |
| for LDP VPLS.....                               | 725, 742                 |
| for VPWS.....                                   | 459, 713                 |
| BGP route reflectors                            |                          |
| VPLS.....                                       | 552                      |
| BGP signaling                                   |                          |
| VPLS.....                                       | 549                      |
| BGP VPLS                                        |                          |
| control word.....                               | 550, 551                 |
| BGP_L2VPN_AD_NLRI.....                          | 1072                     |
| BPDUs, spanning tree.....                       | 923                      |
| BPDUs, nonstandard.....                         | 162                      |
| braces, in configuration statements.....        | xxx                      |
| brackets                                        |                          |
| angle, in syntax descriptions.....              | xxx                      |
| square, in configuration statements.....        | xxx                      |
| bridging domains.....                           | 892                      |
| <b>C</b>                                        |                          |
| CAC.....                                        | 363, 365                 |
| fast reroute.....                               | 365                      |
| link and node protection.....                   | 365                      |
| LSP path protection.....                        | 364                      |
| secondary paths.....                            | 364                      |
| call admission control See CAC                  |                          |
| CCC                                             |                          |
| Frame Relay, control word.....                  | 352                      |
| CE devices, routers or switches.....            | 7                        |
| chained composite next hops.....                | 83                       |
| cisco-non-deterministic option.....             | 169                      |
| class of service See CoS                        |                          |
| clear security group-vpn member ike             |                          |
| security-associations command.....              | 1239                     |
| clear security group-vpn member kek             |                          |
| security-associations command.....              | 1240                     |
| clear vpls mac-address command.....             | 1241                     |
| clear vpls mac-table command.....               | 1243                     |
| comments, in configuration statements.....      | xxx                      |
| communities                                     |                          |
| regular expressions.....                        | 28                       |
| community statement.....                        | 1078                     |
| Layer 2 circuits                                |                          |
| usage guidelines.....                           | 351, 357                 |
| connection-protection.....                      | 1079                     |
| connections                                     |                          |
| testing                                         |                          |
| MPLS Layer 2 circuit connections.....           | 1244                     |
| MPLS Layer 2 VPN connections.....               | 1247                     |
| connectivity-type statement.....                | 1080                     |
| usage guidelines.....                           | 572                      |
| control word                                    |                          |
| BGP VPLS.....                                   | 550, 551                 |
| control word, Frame Relay.....                  | 352                      |
| control-channel statement.....                  | 1081                     |
| usage guidelines.....                           | 188                      |
| control-word statement                          |                          |
| Layer 2 circuits.....                           | 1082                     |
| usage guidelines.....                           | 353                      |
| Layer 2 VPNs.....                               | 1083                     |
| usage guidelines.....                           | 167                      |
| routing-instances.....                          | 1084                     |
| conventions                                     |                          |
| text and syntax.....                            | xxix                     |
| cooloff time.....                               | 900, 901, 903, 904, 1231 |
| CoS                                             |                          |
| VPNs.....                                       | 113                      |
| curly braces, in configuration statements.....  | xxx                      |
| customer edge devices or routers See CE devices |                          |
| customer support.....                           | xxxi                     |
| contacting JTAC.....                            | xxxi                     |
| <b>D</b>                                        |                          |
| description statement.....                      | 1040, 1084, 1085         |
| Designated Forwarder                            |                          |
| election                                        |                          |
| BDF.....                                        | 258                      |
| DF.....                                         | 258                      |
| destination MAC address                         |                          |
| firewall filter match conditions                |                          |
| VPLS traffic.....                               | 926                      |
| detection-time statement.....                   | 1077                     |
| BGP.....                                        | 1086                     |
| usage guidelines.....                           | 186                      |
| DF Election                                     |                          |
| failover.....                                   | 258                      |
| procedure.....                                  | 258                      |
| trigger.....                                    | 258                      |
| documentation                                   |                          |
| comments on.....                                | xxxi                     |
| DoS attack.....                                 | 102                      |
| DSCP code point                                 |                          |
| firewall filter match condition                 |                          |
| VPLS traffic.....                               | 926                      |
| Dynamic Placement of Multisegment Pseudowire    |                          |
| overview.....                                   | 452, 490                 |
| dynamic profiles                                |                          |
| MX Series VPLS examples.....                    | 619, 620, 625            |

**E**

|                                           |            |
|-------------------------------------------|------------|
| egress protection                         |            |
| service mirroring.....                    | 471        |
| egress protection LSP, configuring.....   | 404        |
| egress-protection statement               |            |
| Layer 2 circuits.....                     | 1100       |
| MPLS.....                                 | 1101, 1209 |
| encapsulation mismatch                    |            |
| Layer 2 circuits.....                     | 353        |
| encapsulation statement                   |            |
| logical interfaces.....                   | 1088       |
| usage guidelines (TCC).....               | 164        |
| physical interface.....                   | 1092       |
| physical interfaces                       |            |
| usage guidelines (TCC).....               | 164        |
| VPLS                                      |            |
| usage guidelines.....                     | 604        |
| encapsulation-type statement.....         | 1099       |
| Layer 2 circuits.....                     | 1097       |
| usage guidelines.....                     | 353        |
| VPLS                                      |            |
| usage guidelines.....                     | 573        |
| end-interface statement.....              | 1102       |
| usage guidelines.....                     | 348        |
| esi statement.....                        | 1103       |
| Ethernet interfaces                       |            |
| VLAN tagging.....                         | 1226       |
| EVPN                                      |            |
| IRB solution.....                         | 302        |
| multihoming.....                          | 261        |
| virtual switch.....                       | 327, 331   |
| EVPN Multihoming                          |            |
| active-standby.....                       | 249        |
| active-standby configuration example..... | 264        |
| concepts.....                             | 247        |
| introduction.....                         | 245        |
| operation mode.....                       | 249        |
| overview.....                             | 245        |
| evpn statement                            |            |
| usage guidelines.....                     | 240        |
| EVPNs                                     |            |
| routing instance, configuring.....        | 239        |
| example                                   |            |
| egress protection LSP.....                | 404        |
| export policy, VRF.....                   | 29         |
| extended-vlan-list statement.....         | 1104       |
| external-router-id option.....            | 169        |

**F**

|                                      |                           |
|--------------------------------------|---------------------------|
| family evpn.....                     | 20                        |
| family inet-vpn.....                 | 20                        |
| family inet6-vpn.....                | 20                        |
| family l2vpn.....                    | 20                        |
| family multiservice statement.....   | 1109                      |
| MX Series routers                    |                           |
| usage guidelines.....                | 898                       |
| usage guidelines.....                | 895                       |
| VPLS load balancing                  |                           |
| usage guidelines.....                | 897                       |
| family route-target statement.....   | 1041                      |
| usage guidelines.....                | 38                        |
| family statement                     |                           |
| BGP.....                             | 1105                      |
| Fast Ethernet interfaces             |                           |
| VLAN tagging.....                    | 1226                      |
| fast reroute priority                |                           |
| VPLS.....                            | 577                       |
| fast reroute, CAC.....               | 365                       |
| fast-aps-switch                      |                           |
| configuring.....                     | 395                       |
| fast-aps-switch statement.....       | 1111                      |
| fast-reroute-priority statement..... | 1112                      |
| usage guidelines.....                | 577                       |
| FEC 128                              |                           |
| pseudowire                           |                           |
| load balancing.....                  | 534, 629                  |
| VPLS.....                            | 629                       |
| VPWS.....                            | 534                       |
| FEC 129.....                         | 769, 1072 See multihoming |
| multisegment pseudowire.....         | 452, 489                  |
| pseudowire                           |                           |
| load balancing.....                  | 536, 631                  |
| VPWS.....                            | 459, 536, 713             |
| filters, VPLS.....                   | 921                       |
| firewall filters                     |                           |
| VPLS.....                            | 921                       |
| flexible match mask                  |                           |
| firewall filter match conditions     |                           |
| VPLS traffic.....                    | 926                       |
| flexible match range                 |                           |
| firewall filter match conditions     |                           |
| VPLS traffic.....                    | 926                       |
| flow labels, MPLS.....               | 534, 536, 629, 631        |
| flow statement.....                  | 1105                      |
| flow-label-receive statement         |                           |
| usage guidelines.....                | 534, 536, 629, 631        |
| flow-label-receive-static.....       | 1113                      |

|                                               |                          |
|-----------------------------------------------|--------------------------|
| flow-label-receive-static statement           |                          |
| usage guidelines.....                         | 534                      |
| flow-label-transmit statement                 |                          |
| usage guidelines.....                         | 534, 536, 629, 631       |
| flow-label-transmit-static.....               | 1113                     |
| flow-label-transmit-static statement          |                          |
| usage guidelines.....                         | 534                      |
| font conventions.....                         | xxix                     |
| forwarding class                              |                          |
| firewall filter match conditions              |                          |
| VPLS traffic.....                             | 926                      |
| <b>G</b>                                      |                          |
| Gigabit Ethernet interfaces                   |                          |
| VLAN tagging.....                             | 1226                     |
| graceful-restart statement.....               | 1042                     |
| Group VPN                                     |                          |
| configuring.....                              | 213                      |
| Group VPNs                                    |                          |
| overview.....                                 | 194                      |
| <b>H</b>                                      |                          |
| H-VPLS                                        |                          |
| example.....                                  | 632, 681, 693            |
| hosts, reachability                           |                          |
| MPLS Layer 2 circuits.....                    | 1244                     |
| MPLS Layer 2 VPN connections.....             | 1247                     |
| hot-standby                                   |                          |
| edit routing-instances.....                   | 1114                     |
| hot-standby statement.....                    | 1115                     |
| hot-standby-vc-on statement.....              | 1116                     |
| Hub and spoke VPLS                            |                          |
| VLANs, enabling.....                          | 608                      |
| <b>I</b>                                      |                          |
| ICMP replies, VPLS.....                       | 549                      |
| identifier statement.....                     | 1117                     |
| IFL.....                                      | 1242, 1322               |
| ignore-encapsulation-mismatch statement.....  | 1118                     |
| usage guidelines.....                         | 240, 353                 |
| ignore-mtu-mismatch statement.....            | 1119                     |
| usage guidelines.....                         | 165, 349                 |
| import communities                            |                          |
| regular expressions.....                      | 28                       |
| import policy, VRF.....                       | 27                       |
| in-band signaling                             |                          |
| for multipoint LDP.....                       | 371                      |
| inband signaling                              |                          |
| for multipoint LDP.....                       | 367                      |
| install-nexthop statement.....                | 1126                     |
| usage guidelines.....                         | 358                      |
| instance-type statement.....                  | 1044                     |
| usage guidelines.....                         | 10, 239                  |
| instances, Layer 2 VPN                        |                          |
| overview.....                                 | 447, 708                 |
| integrated routing and bridging.....          | 892                      |
| inter-AS                                      |                          |
| VPLS.....                                     | 559                      |
| Inter-AS VPLS with MAC operations.....        | 559                      |
| interface recovery time.....                  | 900, 901, 903, 904, 1231 |
| interface statement.....                      | 1123                     |
| EVPNs.....                                    | 1120                     |
| usage guidelines.....                         | 240                      |
| IS-IS.....                                    | 1046                     |
| Layer 2 circuits.....                         | 1121                     |
| usage guidelines.....                         | 350                      |
| Layer 2 VPNs.....                             | 1122                     |
| usage guidelines.....                         | 127                      |
| OSPF.....                                     | 1046                     |
| routing instances                             |                          |
| usage guidelines.....                         | 239                      |
| VPLS.....                                     | 1124                     |
| usage guidelines.....                         | 568                      |
| VPNs.....                                     | 1046                     |
| usage guidelines.....                         | 11                       |
| interface-mac-limit statement.....            | 1125                     |
| usage guidelines.....                         | 241, 574                 |
| interfaces descriptive text.....              | 1040                     |
| Internet draft                                |                          |
| draft-kompella-l2vpn-vpls-multihoming-03.txt, |                          |
| Multi-homing in BGP-based Virtual Private LAN |                          |
| Service.....                                  | 123, 542                 |
| IP spoofing.....                              | 102                      |
| IPsec                                         |                          |
| SAs.....                                      | 194                      |
| <i>See also</i> Group VPNs                    |                          |
| IRB                                           |                          |
| VPLS, interface connectivity.....             | 572                      |
| <b>L</b>                                      |                          |
| l2circuit                                     |                          |
| H-VPLS                                        |                          |
| usage guidelines.....                         | 632, 681, 693            |
| l2circuit statement.....                      | 1127                     |
| l2ckt statement.....                          | 1128                     |
| l2vpn statement.....                          | 1129                     |
| usage guidelines.....                         | 127                      |

- l2vpn-id statement.....1132
  - usage guidelines.....725, 742
  - VPWS.....459, 713
- l2vpn-use-bgp-rules statement.....1133
- label blocks example, VPLS.....596
- label blocks operation.....591
- label switching interfaces
  - VPLS.....611
- label-allocation statement.....1133
  - usage guidelines.....241
- label-block-size statement.....1134
- Label-Switched Interface (LSI)
  - status information, displaying.....1258
- label-switched-path-template statement.....1135
  - usage guidelines.....847
- Layer 2 circuits
  - BFD for VCCV.....188
  - CAC.....363
  - connections, displaying.....1261
  - egress protection LSP.....404
  - reachability, testing.....1244
  - redundant pseudowires.....179, 1252
  - supported software standards.....450
- Layer 2 VPN
  - stitching.....945, 947
- Layer 2 VPNs
  - BFD for VCCV.....188
  - connections, displaying.....1269
  - overview.....3
  - path selection.....173
  - reachability, testing.....1247
  - route distinguisher.....13
  - VPLS connections, displaying.....1305
  - VPLS statistics, displaying.....1329
- Layer 2 VPNs, multihoming.....173
- Layer 3 VPNs
  - overview.....4
  - static route target filtering.....82
- layer-3 statement
  - load balancing
    - usage guidelines.....898
- layer-3-only statement
  - usage guidelines.....897
- layer-4 statement
  - load balancing
    - usage guidelines.....898
- Layer 2
  - MTU.....165
- Layer 2 circuits
  - ATM trunking.....361, 365
  - bandwidth accounting.....363
  - BPDUs.....162
  - call admission control.....363
  - encapsulation mismatch.....353
  - local interface switching.....348
  - ping command.....115
  - static pseudowires.....347
  - trunk mode.....365
- Layer 2 VPNs
  - BPDUs.....162
  - configuration example.....132
  - hub-and-spoke topology.....128
  - multihoming.....130, 1157
  - ping command.....115
  - proxy statement to configure a TCC.....165
  - remote statement to configure a TCC.....165
  - site configuration.....127
  - TCC encapsulation.....164
- Layer 2.5 VPNs.....164
- Layer 3 VPNs
  - ping command.....115
- LDP
  - multipoint.....367
- LDP BGP interworking
  - configuration guidelines.....556
  - platform support.....557
  - systems supported.....556
- LDP signaling
  - VPLS.....569
- LDP SP-PE TLV.....454, 491
- LDP VPLS
  - with BGP autodiscovery.....725, 742
- LDP-based Layer 2 VPN and VPLS update
  - messages
    - BGP.....1072
- link and node protection, CAC.....365
- load balancing
  - MPLS.....534, 536, 629, 631
  - VPLS.....895
    - M120 and M320 routers.....897
    - MX Series routers.....898
- local interface switching.....348
- local switching interface
  - MTU.....349

|                                         |                    |  |
|-----------------------------------------|--------------------|--|
| local-switching statement               |                    |  |
| Layer 2 circuits.....                   | 1136               |  |
| usage guidelines.....                   | 348                |  |
| VPLS.....                               | 1137               |  |
| usage guidelines.....                   | 558                |  |
| logical systems                         |                    |  |
| VPNs.....                               | 6                  |  |
| logical-router See logical-system       |                    |  |
| logical-routers See logical-systems     |                    |  |
| loss priority                           |                    |  |
| firewall filter match conditions        |                    |  |
| VPLS traffic.....                       | 926                |  |
| LSI                                     |                    |  |
| VPLS.....                               | 611                |  |
| LSPs                                    |                    |  |
| flow labels.....                        | 534, 536, 629, 631 |  |
| <b>M</b>                                |                    |  |
| MAC address                             |                    |  |
| VPLS limits.....                        | 574                |  |
| mac-flush statement.....                | 1138               |  |
| usage guidelines.....                   | 576                |  |
| mac-statistics statement.....           | 1140               |  |
| usage guidelines.....                   | 241                |  |
| mac-table-aging-time statement.....     | 1142               |  |
| usage guidelines.....                   | 573                |  |
| mac-table-size statement.....           | 1143               |  |
| usage guidelines.....                   | 241, 574           |  |
| manuals                                 |                    |  |
| comments on.....                        | xxxi               |  |
| match conditions for firewall filters   |                    |  |
| VPLS traffic.....                       | 926                |  |
| med-plus-igp statement                  |                    |  |
| usage guidelines.....                   | 169                |  |
| mesh-group statement.....               | 1144               |  |
| configuration guidelines.....           | 556                |  |
| usage guidelines.....                   | 742                |  |
| minimum-interval.....                   | 1146               |  |
| BFD, transmit-interval.....             | 1148               |  |
| minimum-interval statement.....         | 1077               |  |
| usage guidelines.....                   | 186                |  |
| minimum-receive-interval                |                    |  |
| BFD.....                                | 1150               |  |
| minimum-receive-interval statement..... | 1077               |  |
| usage guidelines.....                   | 187                |  |
| mobile backhaul                         |                    |  |
| pseudowire redundancy.....              | 371                |  |
| MP-BGP.....                             | 1105               |  |
| MPLS                                    |                    |  |
| chained composite next hops.....        | 83                 |  |
| flow label, configuration.....          | 534, 536, 629, 631 |  |
| Layer 2 circuit connections             |                    |  |
| operability, checking.....              | 1244               |  |
| Layer 2 VPN connections                 |                    |  |
| operability, checking.....              | 780, 1247          |  |
| load balancing.....                     | 534, 536, 629, 631 |  |
| MSTP, VPLS.....                         | 894                |  |
| MTU                                     |                    |  |
| Layer 2.....                            | 165                |  |
| local switching interface.....          | 349                |  |
| mtu statement.....                      | 1152               |  |
| usage guidelines.....                   | 165                |  |
| multi-homing statement.....             | 1157, 1158         |  |
| FEC 129                                 |                    |  |
| usage guidelines.....                   | 769                |  |
| usage guidelines.....                   | 755                |  |
| multihomed PE routers.....              | 549                |  |
| multihoming                             |                    |  |
| configuration, VPLS.....                | 753                |  |
| Layer 2 VPNs.....                       | 130                |  |
| path selection.....                     | 173                |  |
| VPLS.....                               | 1157               |  |
| VPLS, overview.....                     | 705, 767           |  |
| multiplier                              |                    |  |
| BFD.....                                | 1156               |  |
| multiplier statement.....               | 1077               |  |
| usage guidelines.....                   | 187                |  |
| multipoint                              |                    |  |
| LDP.....                                | 367                |  |
| multiprotocol BGP (MP-BGP).....         | 1105               |  |
| Multisegment Pseudowire                 |                    |  |
| FEC 129 support.....                    | 452, 489           |  |
| overview.....                           | 451, 488           |  |
| Pseudowire status message.....          | 453, 490           |  |
| MX Series                               |                    |  |
| VPLS pseudowires with dynamic           |                    |  |
| profiles.....                           | 619, 620, 625      |  |
| <b>N</b>                                |                    |  |
| neighbor statement.....                 | 1159               |  |
| usage guidelines.....                   | 569                |  |
| VPLS.....                               | 1161               |  |
| NLRI                                    |                    |  |
| BGP_L2VPN_AD_NLRI.....                  | 1072               |  |
| no-adaptation                           |                    |  |
| BFD.....                                | 1163               |  |



- no-adaptation statement.....1077
    - usage guidelines.....187
  - no-control-word statement
    - Layer 2 circuits
      - usage guidelines.....353
    - Layer 2 VPNs.....1165
      - usage guidelines.....167
    - routing-instances.....1164
  - no-forwarding statement.....1047
    - usage guidelines.....15
  - no-l2ckt statement.....1166
  - no-l2vpn statement.....1166
  - no-local-switching statement.....1167
    - configuration guidelines.....893
  - no-mac-learning statement.....1168
    - usage guidelines.....241
  - no-tunnel-services statement.....1172
    - usage guidelines.....611
  - nonstandard BPDUs.....162
  - normal TTL decrementing for VPNs.....132
- O**
- oam statement.....1173
    - usage guidelines.....186
  - OSPF
    - enabling.....1046
- P**
- P routers.....7
  - packet-action statement.....1174
    - usage guidelines.....241
  - parentheses, in syntax descriptions.....xxx
  - Passive role.....452, 490
  - path MTU check, VPNs.....16
  - path selection, Layer 2 VPNs and VPLS.....173
  - path-selection statement
    - usage guidelines.....169
  - payload statement
    - usage guidelines.....897
  - PE routers.....7
  - peer-active statement.....1177
  - peer-as statement.....1178
    - usage guidelines
      - VPLS.....560
  - physical interfaces
    - VLAN tagging.....1226
  - physical interfaces, descriptive text.....1040
  - ping command
    - usage guidelines
      - Layer 2 circuits.....115
      - VPLS.....115
      - VPNs.....115
  - ping mpls l2circuit command.....1244
  - ping mpls l2vpn command.....1247
  - ping vpls instance command.....1250
  - ping-interval statement.....1179
    - usage guidelines.....188
  - policer statement.....1180
  - policers
    - VPLS.....921
  - policy, routing
    - route target prefix list.....1055
  - port number (TCP or UDP), source or destination
    - firewall filter match conditions
      - VPLS traffic.....926
  - preference statement.....1181, 1182
  - preferences
    - active routes.....169
  - primary statement.....1183
  - protect-interface statement.....1184
  - protected-l2circuit statement.....1185
  - protector-interface statement.....1186
  - protector-pe statement.....1186
  - provider edge routers See PE routers
  - provider routers See P routers
  - proxy statement.....1187
    - usage guidelines.....165
  - proxy-generate statement.....1048
    - usage guidelines.....50, 51
  - pseudowire redundancy
    - failure detection.....179
    - mobile backhaul.....371
  - Pseudowire Status support.....453, 490
    - S-PE.....453, 490
    - T-PE.....453, 490
  - Pseudowire TLV support.....454, 491
  - pseudowire-status-tlv statement.....1187
    - usage guidelines.....354
  - pseudowires
    - redundant switchover.....1252
    - static.....347
    - VPLS mesh groups.....558
  - psn-tunnel-endpoint statement.....1188
    - usage guidelines.....355
  - PTX Series Packet Transport Router.....83

**R**

|                                                                                              |          |
|----------------------------------------------------------------------------------------------|----------|
| reducing aps switchover time.....                                                            | 395      |
| layer 2 circuits                                                                             |          |
| configuring.....                                                                             | 395      |
| redundant pseudowires                                                                        |          |
| configuration.....                                                                           | 179      |
| overview.....                                                                                | 177      |
| revert time.....                                                                             | 181      |
| redundant pseudowires, switchover.....                                                       | 1252     |
| regular expressions, import communities.....                                                 | 28       |
| remote statement.....                                                                        | 1189     |
| usage guidelines.....                                                                        | 165      |
| remote-site-id statement.....                                                                | 1189     |
| request l2circuit-switchover command.....                                                    | 1252     |
| revert time                                                                                  |          |
| redundant pseudowires.....                                                                   | 181      |
| revert-time statement.....                                                                   | 1049     |
| usage guidelines.....                                                                        | 181      |
| RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs).....                                   | 236      |
| RFC 4761, Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling..... | 236, 542 |
| RFC 7432, BGP MPLS-Based Ethernet VPN.....                                                   | 236      |
| route distinguisher.....                                                                     | 13, 1053 |
| automatic.....                                                                               | 14       |
| autonomous system number.....                                                                | 13, 240  |
| route reflectors                                                                             |          |
| BGP route target filtering.....                                                              | 37, 41   |
| proxy BGP route target filtering.....                                                        | 50, 51   |
| route target filtering                                                                       |          |
| static.....                                                                                  | 82       |
| route target filtering, BGP.....                                                             | 38       |
| route target prefix list.....                                                                | 1055     |
| route-distinguisher statement.....                                                           | 1051     |
| usage guidelines.....                                                                        | 13       |
| route-distinguisher-id statement.....                                                        | 1053     |
| usage guidelines.....                                                                        | 14       |
| route-target statement                                                                       |          |
| usage guidelines.....                                                                        | 41       |
| route-target-filter statement                                                                |          |
| usage guidelines.....                                                                        | 49, 1054 |
| routes, displaying                                                                           |          |
| active.....                                                                                  | 1292     |
| routing engine, sampling.....                                                                | 11       |
| routing instance name.....                                                                   | 10       |
| routing instance type.....                                                                   | 10       |
| routing instances                                                                            |          |
| router identifier.....                                                                       | 1053     |

|                                  |      |
|----------------------------------|------|
| routing-instances statement..... | 1190 |
| usage guidelines.....            | 239  |
| rsvp-te statement.....           | 1191 |
| usage guidelines.....            | 847  |
| rtf-prefix-list statement.....   | 1055 |
| usage guidelines.....            | 66   |

**S**

|                                                                       |                  |
|-----------------------------------------------------------------------|------------------|
| SAs.....                                                              | 194              |
| <i>See also</i> Group VPNs                                            |                  |
| show evpn instance command.....                                       | 1253             |
| show interfaces lsi (Label-Switched Interface) command.....           | 1258             |
| show l2circuit connections command.....                               | 1261             |
| show l2vpn connections command.....                                   | 1269             |
| show route command.....                                               | 1292             |
| show security group-vpn member ike security-associations command..... | 1298             |
| show security group-vpn member kek security-associations command..... | 1301             |
| show vpls connections command.....                                    | 1305             |
| show vpls flood event-queue command.....                              | 1316             |
| show vpls flood instance command.....                                 | 1318             |
| show vpls flood route command.....                                    | 1320             |
| show vpls mac-table command.....                                      | 1324             |
| show vpls statistics command.....                                     | 1329             |
| single-homed PE routers.....                                          | 549              |
| site configuration                                                    |                  |
| Layer 2 VPNs.....                                                     | 127              |
| VPLS.....                                                             | 565              |
| site statement.....                                                   | 1192, 1193, 1194 |
| Layer 2 VPNs                                                          |                  |
| usage guidelines.....                                                 | 127              |
| VPLS                                                                  |                  |
| usage guidelines.....                                                 | 565              |
| site-identifier statement.....                                        | 1195             |
| Layer 2 VPNs                                                          |                  |
| usage guidelines.....                                                 | 127              |
| VPLS                                                                  |                  |
| usage guidelines.....                                                 | 565              |
| site-preference statement.....                                        | 1196             |
| Layer 2 VPNs                                                          |                  |
| configuration guidelines.....                                         | 130              |
| VPLS                                                                  |                  |
| usage guidelines.....                                                 | 569              |
| site-range statement.....                                             | 1197             |
| source-attachment-identifier statement.....                           | 1198             |
| standby statement.....                                                | 1199             |

- static pseudowires
    - Layer 2 circuits.....347
  - static pseudowires, configuring.....613
  - static route target filtering.....82
  - static route target filtering, VPNs.....49
  - static statement
    - Layer 2 circuits.....1200
    - usage guidelines.....347
    - usage guidelines.....613
    - VPLS.....1201
  - static-mac statement.....1202
    - usage guidelines.....240
  - statistical approach.....900, 901, 903, 904
  - statistical approach wait time.....900, 901, 903, 1231
  - stitching
    - Layer 2 VPNs.....945, 947
  - support, technical See technical support
  - Supported and Unsupported Features.....454, 491
  - switchover-delay statement.....1056
    - usage guidelines.....180
  - syntax conventions.....xxix
- T**
- target-attachment-identifier statement.....1203
- TCC**
- encapsulation
    - Layer 2 VPNs.....164
- technical support**
- contacting JTAC.....xxxi
- template statement**.....1204
  - usage guidelines.....847
- threshold**
- BFD.....1207
  - BGP.....1205
- threshold statement**.....1077
  - usage guidelines.....186
- threshold-count**.....901, 904
- threshold-time**.....901, 904
- traceoptions statement**
- EVPNs.....1210
  - protocols Layer 2 circuit.....1212
  - protocols Layer 2 VPN.....1214
  - usage guidelines.....242
  - VPLS.....1216
- transmit-interval**
- BFD.....1218
- transmit-interval statement**.....1077
  - usage guidelines.....187
- trunk mode**.....365
- TTL decrementing**
- VPNs.....132
- tunnel services PIC**
- VPLS.....611
- tunnel-services statement**.....1220
  - usage guidelines.....579
- U**
- Understanding Multisegment**
- Pseudowire.....451, 488
- unicast reverse path check**.....1057
- unicast RPF**
- example configuration.....103
  - fail filters.....103
  - VPNs.....102
- unicast-reverse-path statement**.....1057
  - usage guidelines.....102, 103
- V**
- VCCV**.....433, 435
  - BFD .....188
- verification**
- IS-IS policy.....857
  - static route.....110
- version**
- BFD.....1221
- version statement**.....1077
  - usage guidelines.....187
- virtual private LAN service** See VPLS
- Virtual Private Wire Service** See VPWS (virtual private wire service Layer 2 VPNs)
- Virtual switch**
- EVPN.....327, 331
- virtual-circuit-id**
- H-VPLS
    - usage guidelines.....632, 681, 693
- virtual-circuit-id statement**.....1222
- virtual-mac**.....901, 904, 1223, 1231
- virtual-router routing instance**
- overview.....5
- VLAN tagging**.....1226
- vlan-id statement**.....1223, 1224
  - usage guidelines.....239
- vlan-id-list statement**.....1225
- vlan-tagging statement**.....1226
- VPLS**
- autodiscovery.....769
  - BFD for VCCV.....188
  - BGP and LDP signaling.....554

|                                      |                |                                               |                |
|--------------------------------------|----------------|-----------------------------------------------|----------------|
| BGP route reflectors.....            | 552            | tunnel services PIC, configuring without..... | 611            |
| BGP signaling.....                   | 549            | VLANs for hub and spoke networks.....         | 608            |
| bridging domains.....                | 892            | VT interfaces, specifying.....                | 579            |
| connections, displaying.....         | 1305           | with LDP and BGP autodiscovery.....           | 725, 742       |
| duplicate ICMP replies.....          | 549            | Y.1731 delay and delay variation.....         | 939            |
| encapsulation type, configuring..... | 573            | VPLS label block size.....                    | 1134           |
| fast reroute priority.....           | 577            | VPLS load balancing                           |                |
| FEC 128                              |                | M120 and M320 routers.....                    | 897            |
| load balancing.....                  | 629            | MX Series routers.....                        | 898            |
| FEC 129                              |                | VPLS pseudowires                              |                |
| load balancing.....                  | 631            | with dynamic profiles on MX                   |                |
| filters.....                         | 921            | Series.....                                   | 619, 620, 625  |
| actions.....                         | 923            | vpls statement                                |                |
| flood traffic.....                   | 924            | routing-instances.....                        | 1227           |
| FTFs.....                            | 923            | VPLS traffic                                  |                |
| interface-specific counters.....     | 923            | match conditions                              |                |
| interfaces.....                      | 924            | firewall filters.....                         | 926            |
| routing instances.....               | 924            | VPLS, multihoming.....                        | 173, 549, 1157 |
| flood filters.....                   | 924            | vpls-id                                       |                |
| inter-AS.....                        | 559            | H-VPLS                                        |                |
| interface connectivity.....          | 572            | usage guidelines.....                         | 632, 681, 693  |
| IRB.....                             | 572            | vpls-id statement.....                        | 1229           |
| label blocks example.....            | 596            | usage guidelines.....                         | 569            |
| label blocks operation.....          | 591            | vpls-id-list statement.....                   | 1230           |
| LDP BGP interworking.....            | 556, 559       | vpls-mac-move.....                            | 1231           |
| LDP signaling.....                   | 569            | vpn-apply-export statement.....               | 1058           |
| load balancing.....                  | 895            | VPNs                                          |                |
| MAC address limits.....              | 574            | CE devices.....                               | 7              |
| MAC address table.....               | 574            | chained composite next hops.....              | 83             |
| MAC table timeout interval.....      | 573            | CoS.....                                      | 113            |
| mesh groups.....                     | 558            | export policy.....                            | 29             |
| MSTP.....                            | 894            | group See Group VPNs                          |                |
| multihomed site configuration.....   | 753            | Group VPN See Group VPNs                      |                |
| multihoming.....                     | 173, 549, 1157 | import policy.....                            | 27             |
| configuration.....                   | 753            | interfaces.....                               | 11             |
| overview.....                        | 705, 767       | Layer 2                                       |                |
| overview.....                        | 4              | supported software standards.....             | 123            |
| path selection.....                  | 173            | logical systems.....                          | 6              |
| ping command.....                    | 115            | P routers.....                                | 7              |
| policers.....                        | 921, 925       | path MTU check.....                           | 16             |
| redundant pseudowires.....           | 179            | PE routers.....                               | 7              |
| route distinguisher.....             | 13             | route distinguisher.....                      | 13             |
| single-homed site configuration..... | 755            | automatic.....                                | 14             |
| single-homing.....                   | 549            | routing instance name.....                    | 10             |
| site configuration.....              | 565            | routing instances                             |                |
| static pseudowires, configuring..... | 613            | path MTU check.....                           | 17             |
| statistics, displaying.....          | 1329           | static route target filtering.....            | 49             |
| supported software standards.....    | 542            | unicast RPF.....                              | 13, 102        |
| testing connectivity.....            | 1250           |                                               |                |

|                                                  |          |
|--------------------------------------------------|----------|
| VPWS                                             |          |
| FEC 128                                          |          |
| load balancing.....                              | 534      |
| FEC 129                                          |          |
| load balancing.....                              | 536      |
| with BGP autodiscovery.....                      | 459, 713 |
| VPWS (virtual private wire service Layer 2 VPNs) |          |
| instances                                        |          |
| overview.....                                    | 447, 708 |
| overview.....                                    | 447, 708 |
| VRF                                              |          |
| export policy.....                               | 29       |
| import policy.....                               | 27       |
| regular expressions.....                         | 28       |
| VRF export policy.....                           | 1058     |
| vrf-export statement.....                        | 1059     |
| vrf-import statement.....                        | 1060     |
| vrf-mtu-check statement.....                     | 1061     |
| usage guidelines.....                            | 16       |
| vrf-target statement.....                        | 1062     |
| VT interfaces                                    |          |
| VPLS.....                                        | 579      |
| <br>Y                                            |          |
| Y.1731 delay and delay variation                 |          |
| VPLS.....                                        | 939      |

