



IP Multicast: LSM Configuration Guide, Cisco IOS Release 15S

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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

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

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

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

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

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

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

© 2012-2013 Cisco Systems, Inc. All rights reserved.



CONTENTS

MLDP-Based MVPN 1

Finding Feature Information 1

Restrictions for MLDP-Based MVPN 1

Information About MLDP-Based MVPN 1

Overview of MLDP-Based MVPN 2

Benefits of MLDP-Based MVPN 3

Initial Deployment of an MLDP-Based MVPN 4

Default MDT Creation 4

LSP Downstream Default MDT Creation 5

LSP Upstream Default MDT Creation 7

PIM Overlay Signaling of VPN Multicast State 9

Data MDT Scenario 10

How to Configure MLDP-Based MVPN 11

Configuring Initial MLDP Settings 11

Configuring an MLDP-Based MVPN 13

Verifying the Configuration of an MLDP-Based MVPN 15

Configuration Examples for MLDP-Based MVPN 17

Example Initial Deployment of an MLDP-Based MVPN 18

Default MDT Configuration 18

PIM Adjacencies 19

MLDP Database Entry--PE-East 19

Label Forwarding Entry--P-Central (Root 1) 20

Data MDT Configuration 21

VRF mroute Table--PE-West 23

LSP-VIF Adjacencies--PE-West 23

MLDP Database Entries 24

LFIB Entry for the Data MDT 24

Example Migration from a PIM with mGRE-Based MVPN to an MLDP-Based MVPN 25

Additional References 25

Feature Information for MLDP-Based MVPN	26
MLDP Filtering	29
Finding Feature Information	31
Prerequisites for MLDP Filtering	33
Information about MLDP Filtering	35
MLDP Filtering	35
MLDP Disable on an Interface	35
How to Configure MLDP Filtering	37
Disabling MLDP on an Interface	37
Filtering MLDP Traffic	38
Mapping S and G Flows to MDT Trees	39
Verifying MLDP Filtering	40
Configuration Examples for MLDP Filtering	43
Example: MLDP Filtering	43
Example: S and G Mappings to Data MDT Tree Numbers	43
Additional References	45
Feature Information for MLDP Filtering	47
HA Support for MLDP	51
Finding Feature Information	53
Prerequisites for HA Support for MLDP	55
Restrictions for HA Support for MLDP	57
Information About HA Support for MLDP	59
How to Monitor HA Support for MLDP	61
Displaying Check Pointed Information	61
Displaying Data MDT Mappings for MLDP on Standby Device	62
Additional References	65
Feature Information for HA Support for MLDP	67
IPv6 Multicast Listener Discovery Protocol	71
Finding Feature Information	71
Information About IPv6 Multicast Listener Discovery Protocol	71
IPv6 Multicast Overview	71
IPv6 Multicast Routing Implementation	72
Multicast Listener Discovery Protocol for IPv6	73
MLD Access Group	74
How to Configure IPv6 Multicast Listener Discovery Protocol	74
Enabling IPv6 Multicast Routing	74

Customizing and Verifying MLD on an Interface	75
Disabling MLD Device-Side Processing	77
Resetting the MLD Traffic Counters	78
Clearing the MLD Interface Counters	79
Configuration Examples for IPv6 Multicast Listener Discovery Protocol	79
Example: Enabling IPv6 Multicast Routing	80
Example: Configuring the MLD Protocol	80
Example: Disabling MLD Router-Side Processing	81
Additional References	81
IPv6 Multicast Listener Discovery Protocol	82
MLD Group Limits	85
Finding Feature Information	85
Information About MLD Group Limits	85
Multicast Listener Discovery Protocol for IPv6	85
How to Implement MLD Group Limits	86
Implementing MLD Group Limits Globally	87
Implementing MLD Group Limits per Interface	87
Configuration Examples for MLD Group Limits	88
Example: Implementing MLD Group Limits	88
Additional References	89
Feature Information for MLD Group Limits	90
MLDP In-Band Signaling/Transit Mode	93
Finding Feature Information	93
Restrictions for MLDP In-Band Signaling	93
Information About MLDP In-Band Signaling/Transit Mode	93
MLDP In-Band Signaling/Transit Mode	93
How to Configure MLDP In-Band Signaling/Transit Mode	94
Enabling In-Band Signaling on a PE Device	94
Additional References	95
Configuration Examples for MLDP In-Band Signaling/Transit Mode	96
Example: In-Band Signaling on PE1	96
Example: In-Band Signaling on PE2	99
Feature Information for MLDP In-Band Signaling/Transit Mode	102



MLDP-Based MVPN

The MLDP-based MVPN feature provides extensions to Label Distribution Protocol (LDP) for the setup of point-to-multipoint (P2MP) and multipoint-to-multipoint (MP2MP) label switched paths (LSPs) for transport in the Multicast Virtual Private Network (MVPN) core network. This feature is supported in IPv4 and IPv6 networks.

- [Finding Feature Information, page 1](#)
- [Restrictions for MLDP-Based MVPN, page 1](#)
- [Information About MLDP-Based MVPN, page 1](#)
- [How to Configure MLDP-Based MVPN, page 11](#)
- [Configuration Examples for MLDP-Based MVPN, page 17](#)
- [Additional References, page 25](#)
- [Feature Information for MLDP-Based MVPN, page 26](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for MLDP-Based MVPN

MLDP-based MVPN is not supported in the same VRF for which MLDP in-band signaling is configured.

Information About MLDP-Based MVPN

- [Overview of MLDP-Based MVPN, page 2](#)
- [Benefits of MLDP-Based MVPN, page 3](#)
- [Initial Deployment of an MLDP-Based MVPN, page 4](#)

Overview of MLDP-Based MVPN

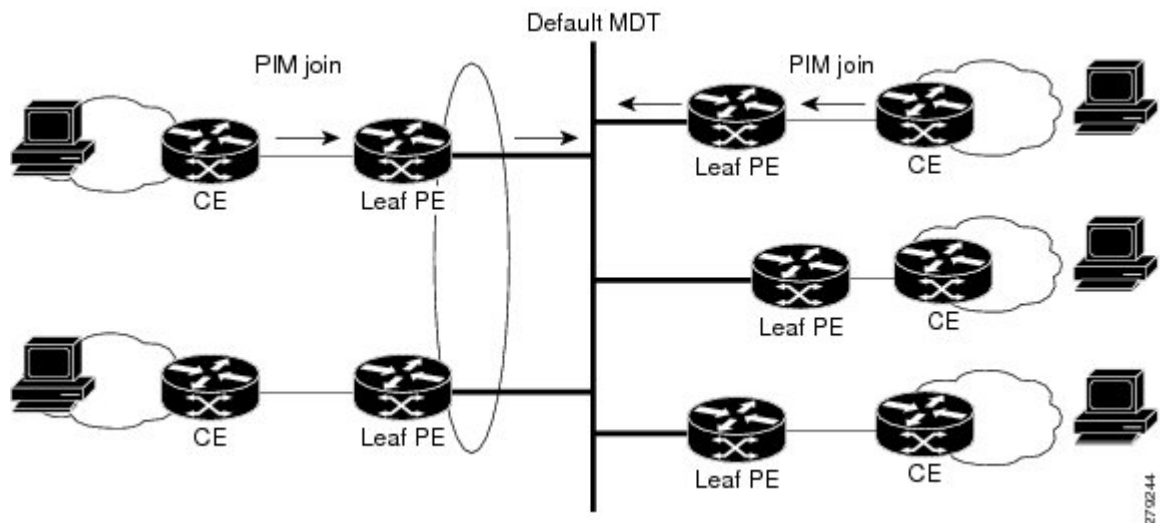
MVPN allows a service provider to configure and support multicast traffic in an MPLS VPN environment. This feature supports routing and forwarding of multicast packets for each individual VPN routing and forwarding (VRF) instance, and it also provides a mechanism to transport VPN multicast packets across the service provider backbone.

A VPN is network connectivity across a shared infrastructure, such as an Internet service provider (ISP). Its function is to provide the same policies and performance as a private network, at a reduced cost of ownership, thus creating many opportunities for cost savings through operations and infrastructure.

An MVPN allows an enterprise to transparently interconnect its private network across the network backbone of a service provider. The use of an MVPN to interconnect an enterprise network in this way does not change the way that the enterprise network is administered, nor does it change general enterprise connectivity.

As shown in the figure, in an MLDP-based MVPN, a static default multicast distribution tree (MDT) is established for each multicast domain. The default MDT defines the path used by provider edge (PE) devices to send multicast data and control messages to every other PE device in the multicast domain. A default MDT is created in the core network using a single MP2MP LSP. The default MDT behaves like a virtual LAN.

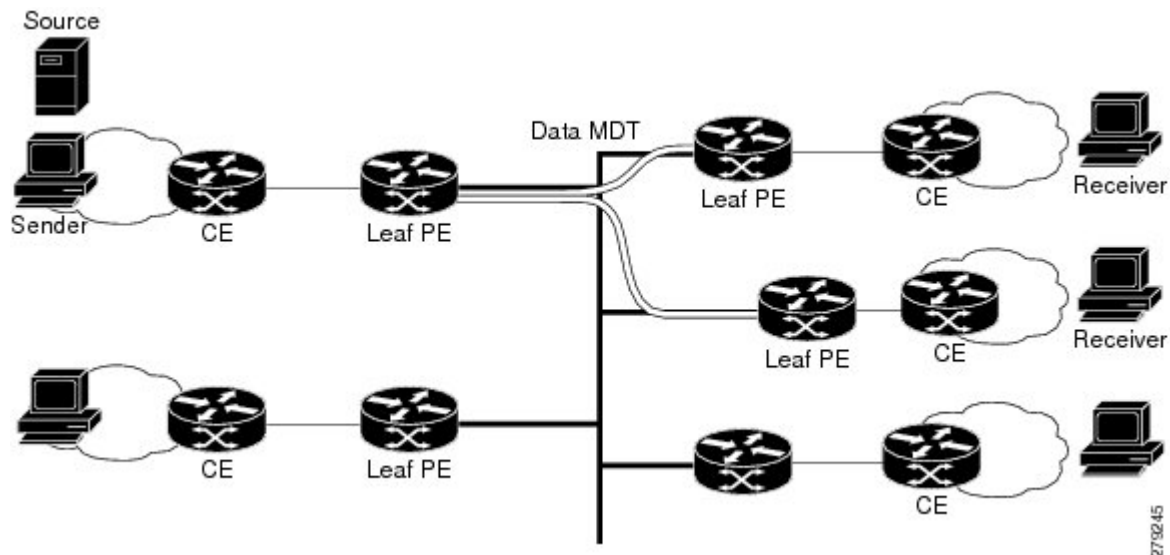
Figure 1 MLDP with the Default MDT Scenario



As shown in the figure, an MLDP-based MVPN also supports the dynamic creation of data MDTs for high-bandwidth transmission. For high-rate data sources, a data MDT is created using P2MP LSPs to off-load traffic from the default MDT to avoid unnecessary waste of bandwidth to PEs that did not join the stream. The creation of the data MDT is signaled dynamically using MDT Join TLV messages. Data MDTs are a feature unique to Cisco IOS software. Data MDTs are intended for high-bandwidth sources such as full-motion video inside the VPN to ensure optimal traffic forwarding in the MPLS VPN core. The threshold at which the data MDT is created can be configured on a per-device or a per-VRF basis. When the multicast transmission exceeds the defined threshold, the sending PE device creates the data MDT and sends a User

Datagram Protocol (UDP) message, which contains information about the data MDT to all devices on the default MDT.

Figure 2 MLDP with the Data MDT Scenario



Data MDTs are created only for (S, G) multicast route entries within the VRF multicast routing table. They are not created for (*, G) entries regardless of the value of the individual source data rate.

The only transport mechanism previously available was Protocol Independent Multicast (PIM) with Multipoint Generic Routing Encapsulation (mGRE) over an IP core network. The introduction of Multicast Label Distribution Protocol (MLDP) provides transport by using MLDP with label encapsulation over an MPLS core network.

MLDP creates the MDTs as follows:

- The default MDT uses MP2MP LSPs.
 - Supports low bandwidth and control traffic between VRFs.
- The data MDT uses P2MP LSPs.
 - Supports a single high-bandwidth source stream from a VRF.

All other operations of MVPN remain the same regardless of the tunneling mechanism:

- PIM neighbors in a VRF are seen across a Label Switched Path virtual interface (LSP-VIF).
- The VPN multicast state is signaled by PIM.

The only other difference when using MLDP is that the MDT group address used in the mGRE solution is replaced with a VPN ID.

Benefits of MLDP-Based MVPN

- Enables the use of a single MPLS forwarding plane for both unicast and multicast traffic.
- Enables existing MPLS protection (for example, MPLS Traffic Engineering/Resource Reservation Protocol (TE/RSVP link protection) and MPLS Operations Administration and Maintenance (OAM) mechanisms) to be used for multicast traffic.

- Reduces operational complexity due to the elimination of the need for PIM in the MPLS core network.

Initial Deployment of an MLDP-Based MVPN

Initial deployment of an MLDP-based MVPN involves the configuration of a default MDT and one or more data MDTs.

A static default MDT is established for each multicast domain. The default MDT defines the path used by PE devices to send multicast data and control messages to every other PE device in the multicast domain. A default MDT is created in the core network using a single MP2MP LSP.

An MLDP-based MVPN also supports the dynamic creation of data MDTs for high-bandwidth transmission.

- [Default MDT Creation, page 4](#)
- [Data MDT Scenario, page 10](#)

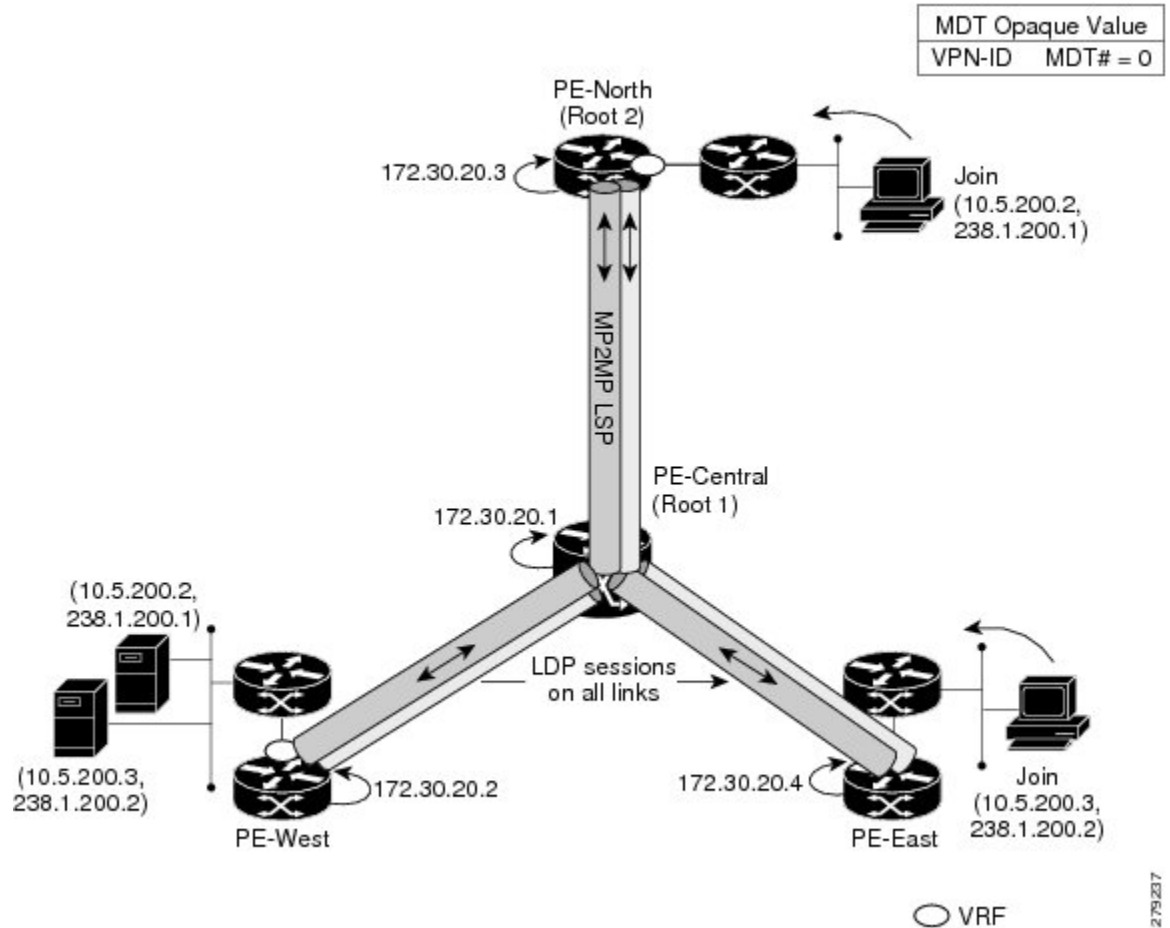
Default MDT Creation

The figure shows the default MDT scenario. The Opaque value used to signal a default MDT consists of two parameters: the VPN ID and the MDT number for the VPN in the format (vpn-id, 0) where vpn-id is a manually configured 7-byte number that uniquely identifies this VPN. The default MDT is set to zero.

In this scenario, each of the three PE devices belong to the VRF called VRF and they have the same VPN ID. Each PE device with the same VPN ID will join the same MP2MP tree. The PE devices have created a primary MP2MP tree rooted at P-Central (Root 1) and a backup MP2MP tree rooted at PE-North (Root 2). There are two sources at PE-West and interested receivers at both PE-North and PE-East. PE-West will

choose one of the MP2MP trees to transmit the customer VPN traffic, but all PE devices can receive traffic on either of the MP2MP trees.

Figure 3 **Default MDT Scenario**



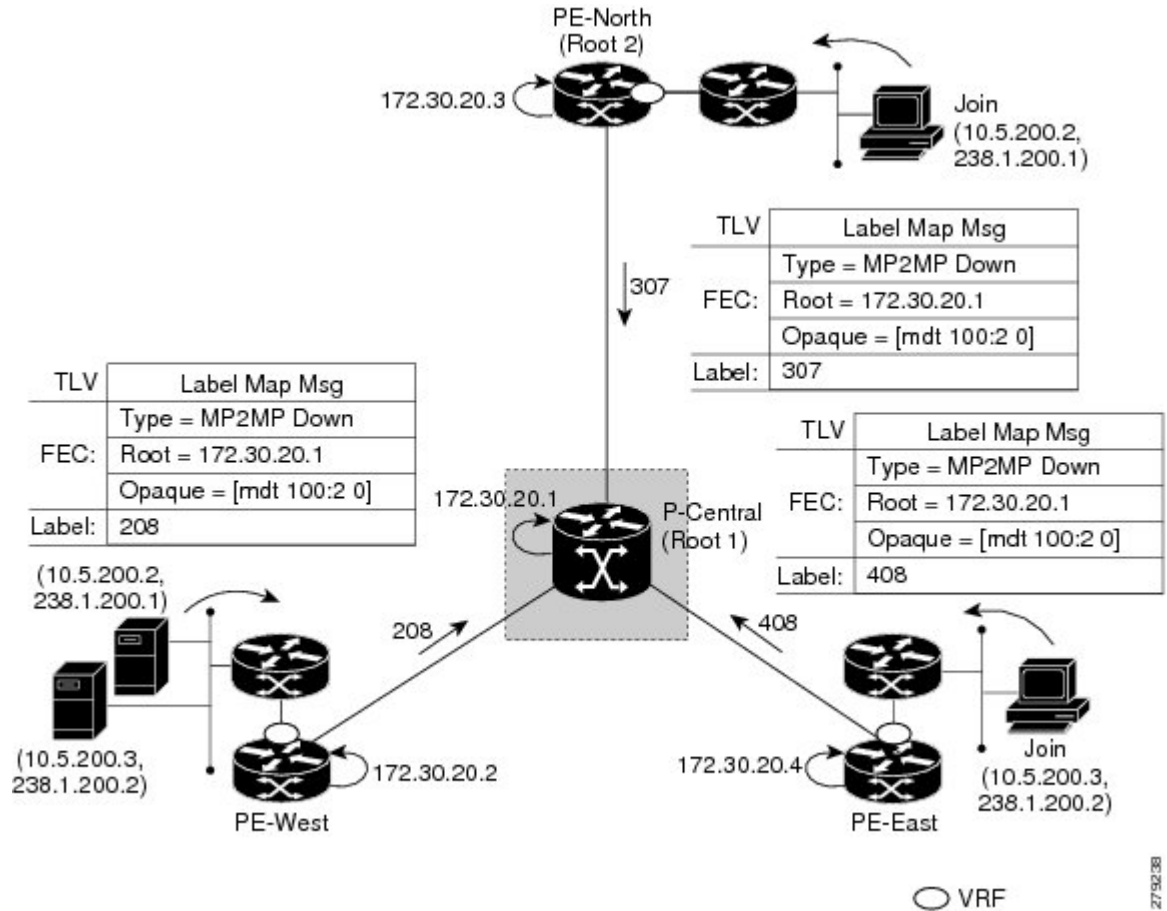
- [LSP Downstream Default MDT Creation, page 5](#)
- [LSP Upstream Default MDT Creation, page 7](#)
- [PIM Overlay Signaling of VPN Multicast State, page 9](#)

LSP Downstream Default MDT Creation

The figures show the downstream tree creation for each of the roots. Each PE device configured with VPN ID 100:2 creates the same Forwarding Equivalence Class (FEC) Type Length Value (TLV), but with a different root and downstream labels per MP2MP tree. The FEC type will be MP2MP Down, which

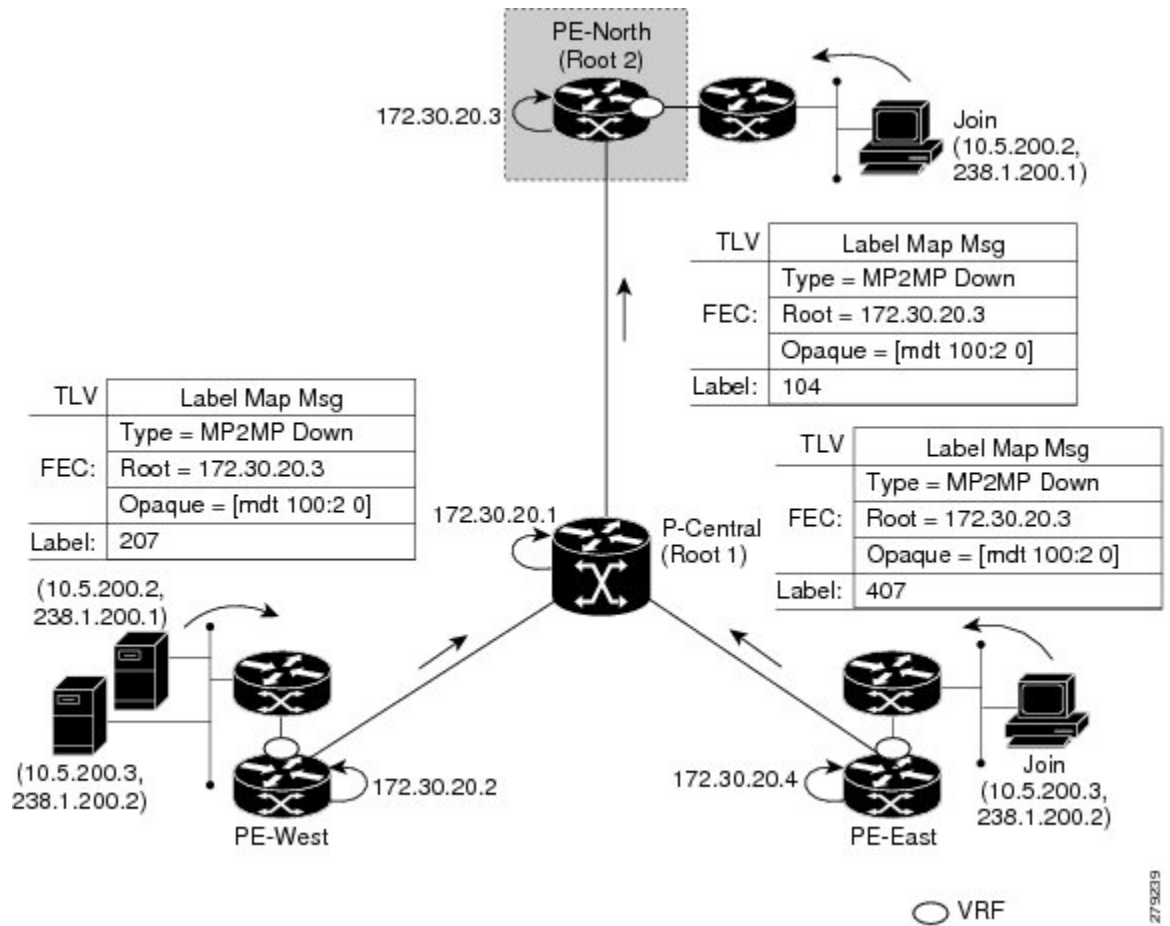
prompts the receiving Label Switched Route (LSR) to respond with an upstream label mapping message to create the upstream path.

Figure 4 **Default MDT Downstream--Root 1**



27/92/38

Figure 5 Default MDT Downstream--Root 2

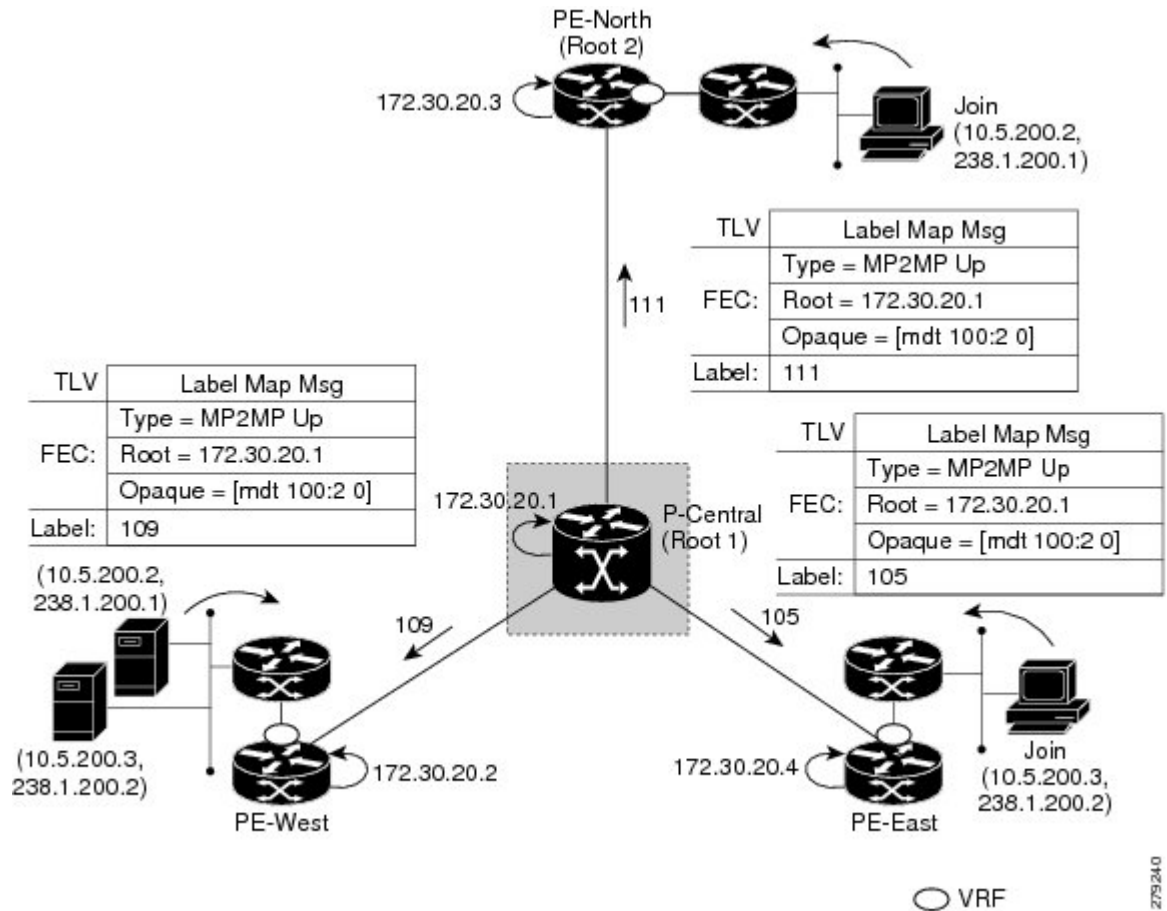


LSP Upstream Default MDT Creation

The figures show the upstream LSP creation for the default MDTs. For each downstream label received, a corresponding upstream label is sent. In the first figure, P-Central sends out three upstream labels (111, 109, and 105) to each downstream directly connected neighbor (downstream is away from the root). The

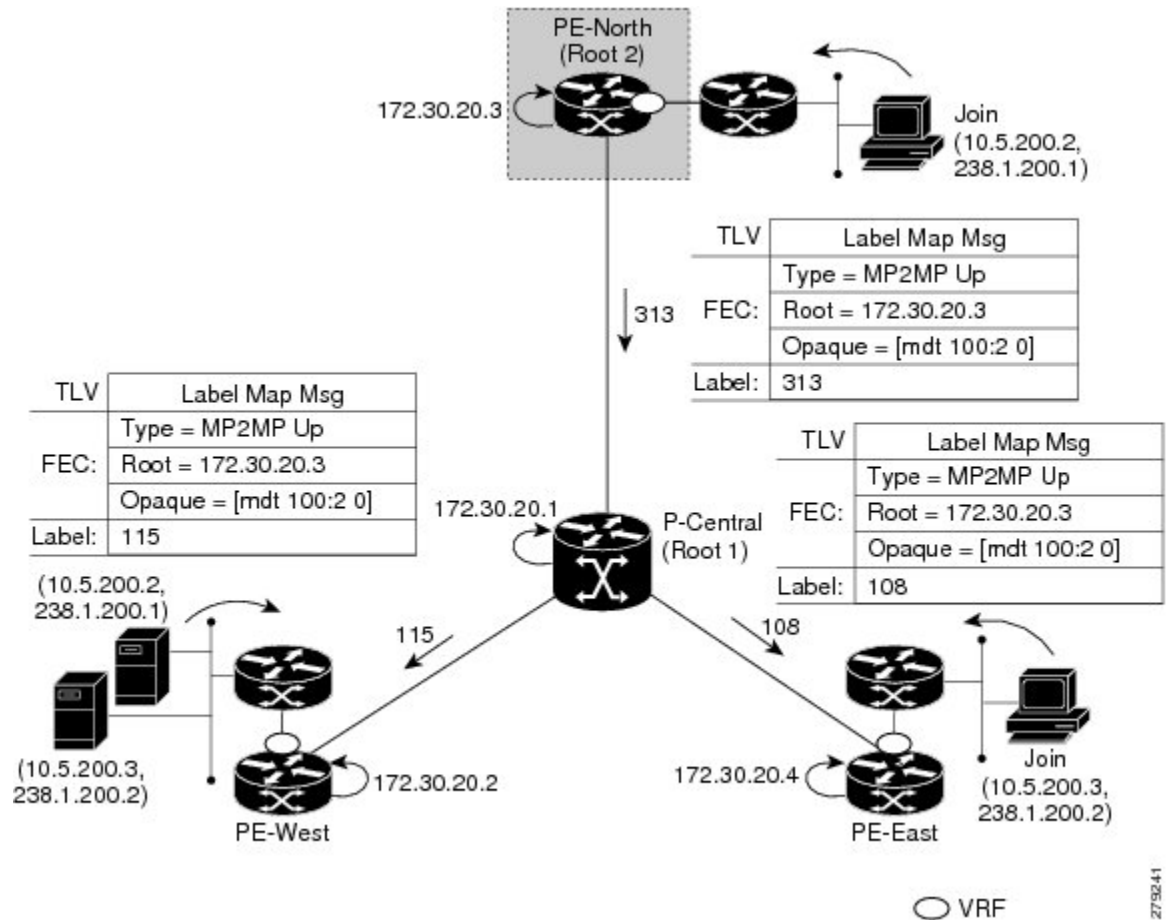
process for PE-North is the same except that it only sends a single upstream label (313) as there is only one directly connected downstream neighbor, as shown in the second figure.

Figure 6 Default MDT Upstream--Root 1



279240

Figure 7 Default MDT Upstream--Root 2

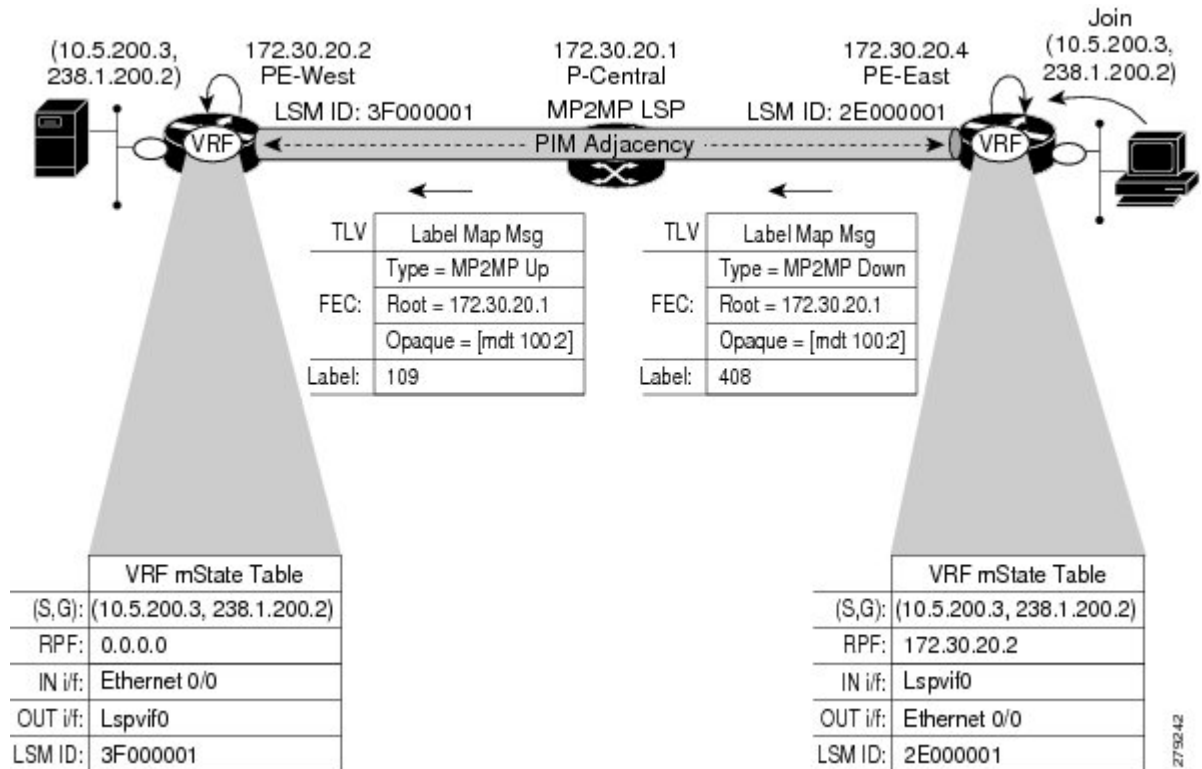


PIM Overlay Signaling of VPN Multicast State

The signaling of the multicast state within a VPN is via PIM. It is called overlay signaling because the PIM session runs over the multipoint LSP and maps the VPN multicast flow to the LSP. In an MVPN, the operation of PIM is independent of the underlying tunnel technology. In the MVPN solution, a PIM adjacency is created between PE devices, and the multicast states within a VRF are populated over the PIM sessions. When using MLDP, the PIM session runs over an LSP-VIF interface. The figure shows PIM signaling running over the default MDT MP2MP LSP. Access to the MP2MP LSP is via the LSP-VIF, which can see all the leaf PE devices at the end of branches, much like a LAN interface. In the figure, PE-East sends a downstream label mapping message to the root, P-Central, which in turn sends an upstream label mapping message to PE-West. These messages result in the creation of the LSP between the two leaf PE devices. A PIM session can then be activated over the top of the LSP allowing the (S, G) states and control messages to be signaled between PE-West and PE-East. In this case, PE-East receives a Join TLV message for (10.5.200.3, 238.1.200.2) within VRF, which it inserts into the mroute table. The Join TLV

message is then sent via the PIM session to PE-West (BGP next-hop of 10.5.200.3), which populates its VRF mroute table. This procedure is identical to the procedure using an mGRE tunnel.

Figure 8 PIM Signaling over LSP



275642

Data MDT Scenario

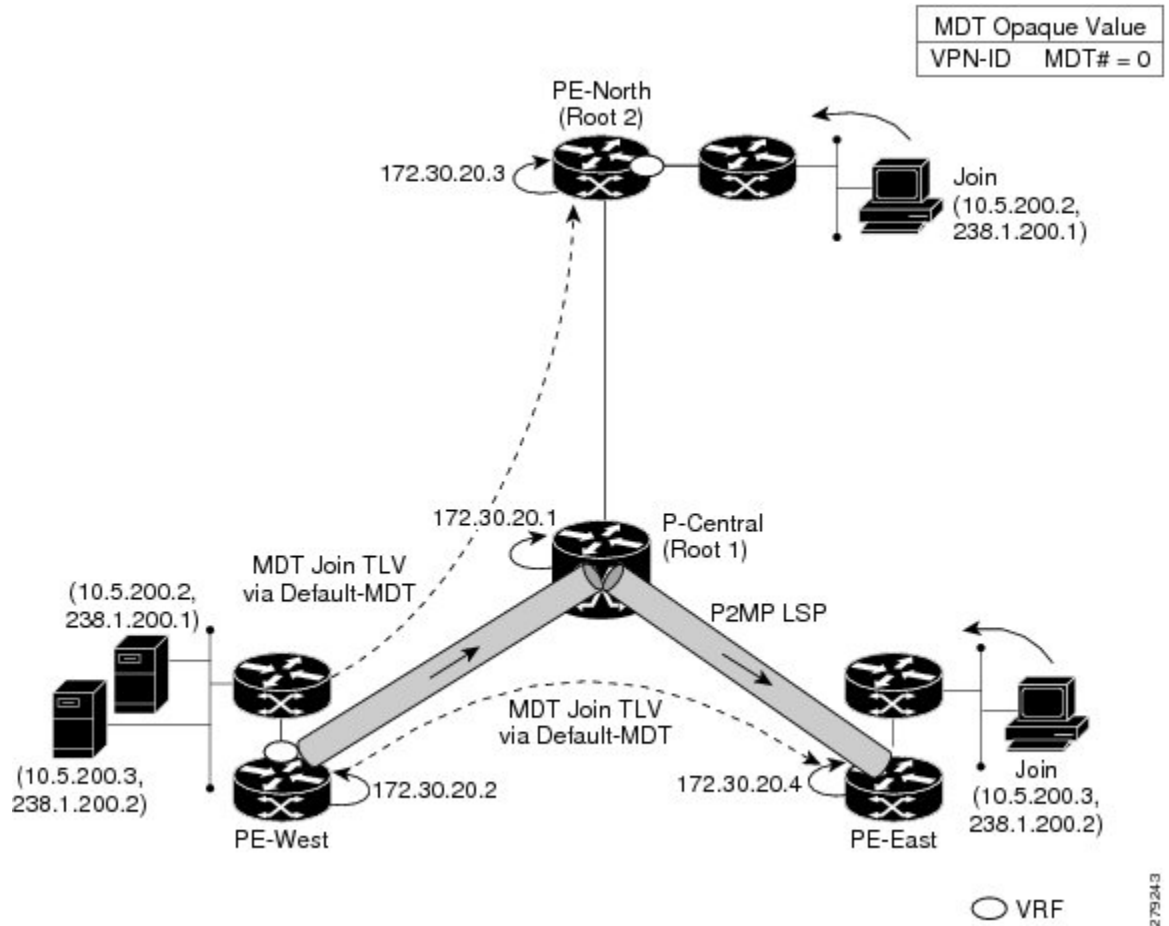
In an MVPN, traffic that exceeds a certain threshold can move off the default MDT onto a data MDT.

The figure shows the data MDT scenario. The Opaque value used to signal a data MDT consists of two parameters: the VPN ID and the MDT number in the format (vpn-id, MDT# > 0) where vpn-id is a manually configured 7-byte number that uniquely identifies this VPN. The second parameter is the unique data MDT number for this VPN, which is a number greater than zero.

In the scenario, two receivers at PE-North and PE-East are interested in two sources at PE-West. If the source 10.5.200.3 exceeds the threshold on the default MDT, PE-West will issue an MDT Join TLV message over the default MDT MP2MP LSP advising all PE devices that a new data MDT is being created.

Because PE-East has an interested receiver in VRF, it will build a multipoint LSP using P2MP back to PE-West, which will be the root of the tree. PE-North does not have a receiver for 10.5.200.3, therefore it will just cache the Join TLV message.

Figure 9 Data MDT Scenario



279243

How to Configure MLDP-Based MVPN

- [Configuring Initial MLDP Settings](#), page 11
- [Configuring an MLDP-Based MVPN](#), page 13
- [Verifying the Configuration of an MLDP-Based MVPN](#), page 15

Configuring Initial MLDP Settings

Perform this task to configure the initial MLDP settings.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls mldp logging notifications**
4. **mpls mldp forwarding recursive**
5. **mpls mldp path { multipath { downstream| upstream} traffic-eng }**
6. **end**

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 enable</p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
<p>Step 2 configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 mpls mldp logging notifications</p> <p>Example:</p> <pre>Device(config)# mpls mldp logging notifications</pre>	<p>Enables MLDP logging notifications.</p>
<p>Step 4 mpls mldp forwarding recursive</p> <p>Example:</p> <pre>Device(config)# mpls mldp forwarding recursive</pre>	<p>Enables MLDP recursive forwarding over a P2MP LSP.</p>
<p>Step 5 mpls mldp path { multipath { downstream upstream} traffic-eng }</p> <p>Example:</p> <pre>Device(config)# mpls mldp path multipath downstream</pre>	<p>Enables load balancing of different LSPs over the available paths or Traffic Engineering (TE) tunnels.</p>

Command or Action	Purpose
Step 6 <code>end</code> Example: Device(config)# <code>end</code>	Ends the current configuration session and returns to privileged EXEC mode.

Configuring an MLDP-Based MVPN

Perform this task to configure an MLDP-based MVPN.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip multicast-routing`
4. `ip multicast-routing vrf vrf-name`
5. `ip vrf vrf-name`
6. `rd route-distinguisher`
7. `vpn id oui : vpn-index`
8. `route target export route-target-ext-community`
9. `route target import route-target-ext-community`
10. `mdt preference { mldp | pim }`
11. `mdt default mpls mldp group-address`
12. `mdt data mpls mldp number-of-data-mdt`
13. `mdt data threshold kb/s list access-list`
14. `end`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: Device# <code>configure terminal</code>	Enters global configuration mode.

	Command or Action	Purpose
Step 3	ip multicast-routing Example: Device(config)# ip multicast-routing	Enables IP multicast routing.
Step 4	ip multicast-routing vrf vrf-name Example: Device(config)# ip multicast-routing vrf VRF	Enables IP multicast routing for the MVPN VRF specified for the <i>vrf-name</i> argument.
Step 5	ip vrf vrf-name Example: Device(config-vrf)# ip vrf VRF	Defines a VRF instance and enters VRF configuration mode.
Step 6	rd route-distinguisher Example: Device(config-vrf)# rd 50:11	Creates a route distinguisher (RD) (in order to make the VRF functional). Creates the routing and forwarding tables, associates the RD with the VRF instance, and specifies the default RD for a VPN.
Step 7	vpn id oui : vpn-index Example: Device(config-vrf)# vpn id 50:10	Sets or updates the VPN ID on a VRF instance.
Step 8	route target export route-target-ext-community Example: Device(config-vrf)# route target export 100:100	Creates an export route target extended community for the specified VRF.
Step 9	route target import route-target-ext-community Example: Device(config-vrf)# route target import 100:100	Creates an import route target extended community for the specified VRF.

Command or Action	Purpose
<p>Step 10 <code>mdt preference { mldp / pim }</code></p> <p>Example:</p> <pre>Device(config-vrf)# mdt preference mldp</pre>	<p>Specifies a preference for a particular MDT type (MLDP or PIM).</p>
<p>Step 11 <code>mdt default mpls mldp group-address</code></p> <p>Example:</p> <pre>Device(config-vrf)# mdt default mpls mldp 172.30.20.1</pre>	<p>Configures a default MDT group for a VPN VRF instance.</p>
<p>Step 12 <code>mdt data mpls mldp number-of-data-mdt</code></p> <p>Example:</p> <pre>Device(config-vrf)# mdt data mpls mldp 255</pre>	<p>Specifies a range of addresses to be used in the data MDT pool.</p>
<p>Step 13 <code>mdt data threshold kb/s list access-list</code></p> <p>Example:</p> <pre>Device(config-vrf)# mdt data threshold 40 list 1</pre>	<p>Defines the bandwidth threshold value in kilobits per second.</p>
<p>Step 14 <code>end</code></p> <p>Example:</p> <pre>Device(config)# end</pre>	<p>Ends the current configuration session and returns to privileged EXEC mode.</p>

Verifying the Configuration of an MLDP-Based MVPN

Perform this task in privileged EXEC mode to verify the configuration of an MLDP-based MVPN.

SUMMARY STEPS

1. show mpls mldp database
2. show ip pim neighbor [vrf vrf-name] neighbor [interface-type interface-number]
3. show ip mroute [vrf vrf-name] [[active [kpbs] [interface type number] | bidirectional | count [terse] | dense | interface type number | proxy | pruned | sparse | ssm | static | summary] | [group-address [source-address]] [count [terse] | interface type number | proxy | pruned | summary] | [source-address group-address] [count [terse] | interface type number | proxy | pruned | summary] | [group-address] active [kpbs] [interface type number | verbose]]
4. show mpls forwarding-table [network {mask | length} | labels label [- label] | interface interface | next-hop address | lsp-tunnel [tunnel-id]] [vrf vrf-name] [detail]
5. show adjacency [ip-address] [interface-type interface-number | null number | port-channel number | sysclock number | vlan number | ipv6-address | fcpa number | serial number] [connectionid number] [link {ipv4 | ipv6 | mpls}] [detail | encapsulation]

DETAILED STEPS

Step 1

show mpls mldp database

Enter the **show mpls mldp database** command to display information in the MLDP database. It shows the FEC, the Opaque value of the FEC decoded, and the replication clients associated with it:

Example:

```
Device# show mpls mldp database
* Indicates MLDP recursive forwarding is enabled
LSM ID : D3000001 (RNR LSM ID: 8A000002)   Type: MP2MP   Uptime : 00:04:54
FEC Root      : 172.30.20.1
Opaque decoded : [mdt 100:2 0]
Opaque length  : 11 bytes
Opaque value   : 07 000B 0000010000000100000000
RNR active LSP : (this entry)
Upstream client(s) :
  172.30.20.1:0 [Active]
    Expires      : Never           Path Set ID   : 99000001
    Out Label (U) : 32             Interface     : Ethernet1/0*
    Local Label (D) : 30           Next Hop      : 10.0.1.7
Replication client(s):
  MDT (VRF VRF)
    Uptime       : 00:04:54       Path Set ID   : 5000002
    Interface    : Lspvif0
```

Step 2

show ip pim neighbor [vrf vrf-name] neighbor [interface-type interface-number]

Enter the **show ip pim neighbor** command to display PIM adjacencies information:

Example:

```
Device# show ip pim vrf VRF neighbor
192.168.10.18   Serial6/0      04:53:19/00:01:18 v2 1 / G
172.30.20.3     Lspvif0       04:52:32/00:01:28 v2 1 / B S P G
172.30.20.2     Lspvif0       04:52:32/00:01:17 v2 1 / B S P G
```

Step 3

show ip mroute [vrf vrf-name] [[active [kpbs] [interface type number] | bidirectional | count [terse] | dense | interface type number | proxy | pruned | sparse | ssm | static | summary] | [group-address [source-address]] [count [terse] | interface type number | proxy | pruned | summary] | [source-address group-address] [count [terse] |

interface *type number* | **proxy** | **pruned** | **summary**] | [*group-address*] **active** [*kbits*] [**interface** *type number* | **verbose**]]

Enter the **show ip mroute** command to display the contents of the multicast routing (mroute) table:

Example:

```
Device# show ip mroute vrf VRF 238.1.200.2 10.5.200.3
(10.5.200.3, 238.1.200.2), 04:54:18/00:02:40, flags: sT
Incoming interface: Lspvif0, RPF nbr 172.30.20.2
Outgoing interface list:
Serial6/0, Forward/Sparse-Dense, 04:54:18/00:02:40
```

Step 4 **show mpls forwarding-table** [*network {mask | length}*] | **labels** *label* [- *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*] | [**vrf** *vrf-name*] [**detail**]

Enter the **show mpls forwarding-table** command to display the contents of the MPLS Label Forwarding Information Base (LFIB):

Example:

```
Device# show mpls forwarding-table | inc 1F000001
105 307 mLDP:1F000001 38468 Se5/0 point2point
    208 mLDP:1F000001 38468 Se4/0 point2point
109 307 mLDP:1F000001 34738 Se5/0 point2point
    408 mLDP:1F000001 34738 Se6/0 point2point
111 408 mLDP:1F000001 282 Se6/0 point2point
    208 mLDP:1F000001 282 Se4/0 point2point
```

Step 5 **show adjacency** [*ip-address*] [*interface-type interface-number*] | **null** *number* | **port-channel** *number* | **sysclock** *number* | **vlan** *number* | *ipv6-address* | **fcpa** *number* | **serial** *number*] [**connectionid** *number*] [**link** {**ipv4** | **ipv6** | **mpls**}] [**detail** | **encapsulation**]

Enter the **show adjacency** command to display adjacency information for the specified LSP-VIF interface:

Example:

```
Device# show adjacency lspvif0
105 307 mLDP:1F000001 38468 Se5/0 point2point
    208 mLDP:1F000001 38468 Se4/0 point2point
109 307 mLDP:1F000001 34738 Se5/0 point2point
    408 mLDP:1F000001 34738 Se6/0 point2point
111 408 mLDP:1F000001 282 Se6/0 point2point
    208 mLDP:1F000001 282 Se4/0 point2point
```

Configuration Examples for MLDP-Based MVPN

- [Example Initial Deployment of an MLDP-Based MVPN, page 18](#)
- [Example Migration from a PIM with mGRE-Based MVPN to an MLDP-Based MVPN, page 25](#)

Example Initial Deployment of an MLDP-Based MVPN

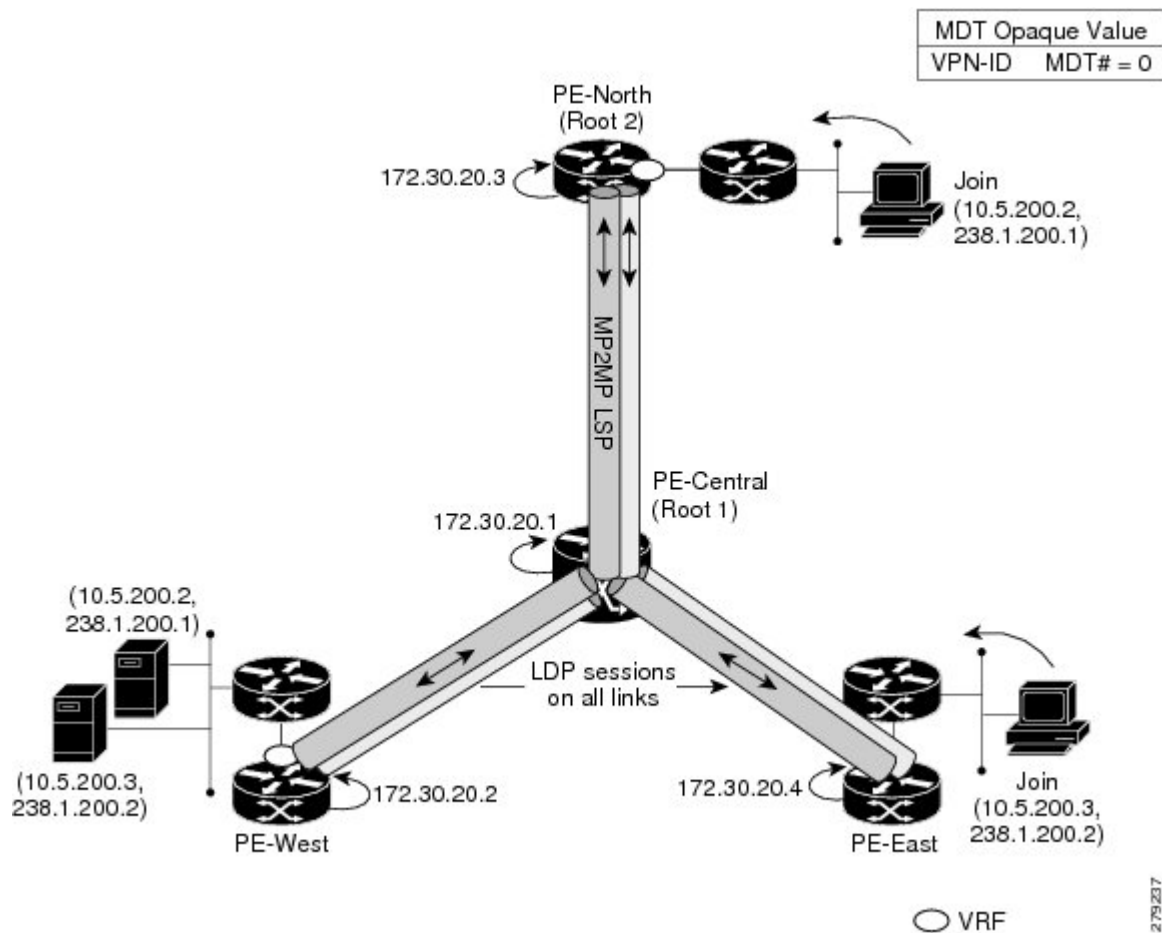
Initial deployment of an MLDP-based MVPN involves the configuration of a default MDT and one or more data MDTs.

- [Default MDT Configuration, page 18](#)
- [Data MDT Configuration, page 21](#)

Default MDT Configuration

The following example shows how to configure the default MDT for an MLDP-based MVPN. This configuration is based on the sample topology illustrated in the figure.

Figure 10 Default MDT Example



This configuration is consistent for every PE device participating in the same VPN ID. The `vpn id 100:2` command replaces the MDT group address used with the mGRE transport method. To provide redundancy, two default MDT trees are statically configured, rooted at P-Central and PE-North. The selection as to

which MP2MP tree the default MDT will use at a particular PE device is determined by Interior Gateway Protocol (IGP) metrics. An MP2MP LSP is implicit for the default MDT.

```
ip pim mpls source Loopback0
ip multicast-routing
ip multicast-routing vrf VRF
!
ip vrf VRF
 rd 100:2
  vpn id 100:2
  route-target export 200:2
  route-target import 200:2
 mdt default mpls mldp 172.30.20.1 (P-Central)
 mdt default mpls mldp 172.30.20.3 (PE-North)
```

- [PIM Adjacencies, page 19](#)
- [MLDP Database Entry--PE-East, page 19](#)
- [Label Forwarding Entry--P-Central \(Root 1\), page 20](#)

PIM Adjacencies

PIM operates over the LSP-VIF as if it were a regular tunnel interface. That means PIM hellos are exchanged over the LSP-VIF to establish PIM adjacencies over the default MDT. The sample output in this section displays the three PIM adjacencies in VRF of PE-East. The first is the adjacency to the receiver network over serial interface 6/0, and the next two are the adjacencies to PE-West and PE-North over the MP2MP LSP via LSP-VIF interface 0.

```
PE-East# show ip pim vrf VRF neighbor
192.168.10.18      Serial6/0          04:53:19/00:01:18 v2 1 / G
172.30.20.3       Lspvif0           04:52:32/00:01:28 v2 1 / B S P G
172.30.20.2       Lspvif0           04:52:32/00:01:17 v2 1 / B S P G
```

The output from the **show ip mroute** command also shows the (S, G) entry for VRF. The stream 238.1.200.2 has the Reverse Path Forwarding (RPF) interface of LSP-VIF interface 0 and the neighbor 172.30.20.2, which is PE-West.

```
PE-East# show ip mroute vrf VRF 238.1.200.2 10.5.200.3
(10.5.200.3, 238.1.200.2), 04:54:18/00:02:40, flags: sT
Incoming interface: Lspvif0, RPF nbr 172.30.20.2
Outgoing interface list:
Serial6/0, Forward/Sparse-Dense, 04:54:18/00:02:40
```

MLDP Database Entry--PE-East

The sample output in this section displays the database entries for the MP2MP trees supporting the default MDT at PE-East. The database is searched by Opaque value MDT 100:2, which results in information for two MP2MP trees (one for each root) being returned. Both trees have different system IDs (2E000001, F2000005) and use the same Opaque value ([mdt 100:2 0]), but with different roots. The last 0 in the Opaque value indicates this tree is a default MDT. Entry 79000004 shows it is the primary MP2MP tree, therefore PE-East will transmit all source multicast traffic on this LSP, and B2000006 will be the backup root. Note that interface LSP-VIF interface 0 represents both MP2MP LSPs. The Local Label (D) is the downstream label allocated by PE-East for this tree. In other words, traffic from the root will be received with either label 408 (Primary Tree) or 407 (Backup Tree). The Out Label (U) is the label that PE-East will use to send traffic into the tree; upstream towards the root, either 105 for the Primary Tree or 108 for the Backup Tree. Both these labels were received from P-Central.

```
PE-East# show mpls mldp database opaque_type mdt 100:2
* Indicates MLDP recursive forwarding is enabled
LSM ID : 79000004 (RNR LSM ID: 8A000002)   Type: MP2MP   Uptime : 00:04:54
```

```

FEC Root          : 172.30.20.1
Opaque decoded    : [mdt 100:2 0]
Opaque length     : 11 bytes
Opaque value      : 07 000B 0000010000000100000000
RNR active LSP    : (this entry)
Upstream client(s) :
  172.30.20.1:0   [Active]
    Expires       : Never           Path Set ID   : 99000001
    Out Label (U) : 32             Interface     : Ethernet1/0*
    Local Label (D): 30           Next Hop      : 10.0.1.7
Replication client(s):
  MDT (VRF VRF)
    Uptime        : 00:04:54       Path Set ID   : 5000002
    Interface     : Lspvif0
LSM ID : 79000005 (RNR LSM ID: 8A000003)   Type: MP2MP   Uptime : 00:04:54
FEC Root          : 172.30.20.3
Opaque decoded    : [mdt 100:2 0]
Opaque length     : 11 bytes
Opaque value      : 07 000B 0000010000000100000001
RNR active LSP    : (this entry)
Upstream client(s) :
  172.30.20.1:0   [Active]
    Expires       : Never           Path Set ID   : 99000002
    Out Label (U) : 32             Interface     : Ethernet1/0*
    Local Label (D): 30           Next Hop      : 10.0.1.7
Replication client(s):
  MDT (VRF VRF)
    Uptime        : 00:04:54       Path Set ID   : 5000003
    Interface     : Lspvif0

```

Label Forwarding Entry--P-Central (Root 1)

The sample output shown in this section displays the VRF (MDT 100:2) MLDP database entry 1F000001 for the primary MP2MP LSP, which is P-Central. Because the local device P-Central is the root, there is no upstream peer ID, therefore no labels are allocated locally. However there are three replication clients, representing each of the three PE devices: PE-North, PE-West, and PE-East. These replication clients are the downstream nodes of the MP2MP LSP. These clients receive multipoint replicated traffic.

In the replication entry looking from the perspective of the root, there are two types of labels:

- Out label (D)--These are labels received from remote peers that are downstream to the root (remember traffic flows downstream away from the root).
- Local label (U)--These are labels provided by P-Central to its neighbors to be used as upstream labels (sending traffic to the root). It is easy to identify these labels as they all start in the 100 range, which we have configured for P-Central to use. P-Central sends these labels out when it receives a FEC with the type as MP2MP Down.

From the labels received and sent in the replication entries, the Label Forwarding Information Base (LFIB) is created. The LFIB has one entry per upstream path and one entry per downstream path. In this case because P-Central is the root, there are only upstream entries in the LFIB that have been merged with the corresponding downstream labels. For example, label 105 is the label P-Central sent to PE-East to send source traffic upstream. Traffic received from PE-East will then be replicated using the downstream labels 307 to PE-West and 208 to PE-North.

```

P-Central# show mpls mldp database opaque_type mdt 100:2
LSM ID : 79000006 (RNR LSM ID: 1F000001)   Type: MP2MP   Uptime : 00:04:54
FEC Root          : 172.30.20.1
Opaque decoded    : [mdt 100:2 0]
Opaque length     : 11 bytes
Opaque value      : 07 000B 0000010000000100000000
RNR active LSP    : (this entry)
Upstream client(s) : None
Replication client(s):
  172.3.20.2:0
    Uptime        : 01:46:43       Path Set ID   : AC000008

```

```

      Out label (D) : 208                Interface   : Serial4/0
      Local label (U): 109                Next Hop    : 172.30.10.2
172.3.20.3:0
      Uptime       : 01:42:43            Path Set ID : E00000C
      Out label (D) : 307                Interface   : Serial5/0
      Local label (U): 111                Next Hop    : 172.30.10.6
172.3.20.4:0
      Uptime       : 01:40:43            Path Set ID : 3D000010
      Out label (D) : 408                Interface   : Serial6/0
      Local label (U): 105                Next Hop    : 172.30.10.10
P-Central# show mpls forwarding-table | inc 1F000001
105  307      mLDP:1F000001    38468      Se5/0      point2point
      208      mLDP:1F000001    38468      Se4/0      point2point
109  307      mLDP:1F000001    34738      Se5/0      point2point
      408      mLDP:1F000001    34738      Se6/0      point2point
111  408      mLDP:1F000001     282       Se6/0      point2point
      208      mLDP:1F000001     282       Se4/0      point2point

```

The sample output shown in this section displays the entry on P-Central for the MP2MP LSP rooted at PE-North (backup root). In this tree P-Central is a branch of the tree, not a root, therefore there are some minor differences to note:

- The upstream peer ID is PE-North, therefore P-Central has allocated label 104 in the downstream direction towards PE-North and subsequently PE-North has responded with an upstream label of 313.
- Two replication entries representing PE-East and PE-West are displayed.
- The merged LFIB shows three entries:
 - One downstream entry label 104 receiving traffic from Root 2 (PE-North), which is then directed further downstream using labels 207 PE-West and 407 PE-East.
 - Two upstream entries 108 and 115 receiving traffic from the leaves and directing it either downstream 207, 407 or upstream using label 313.

```

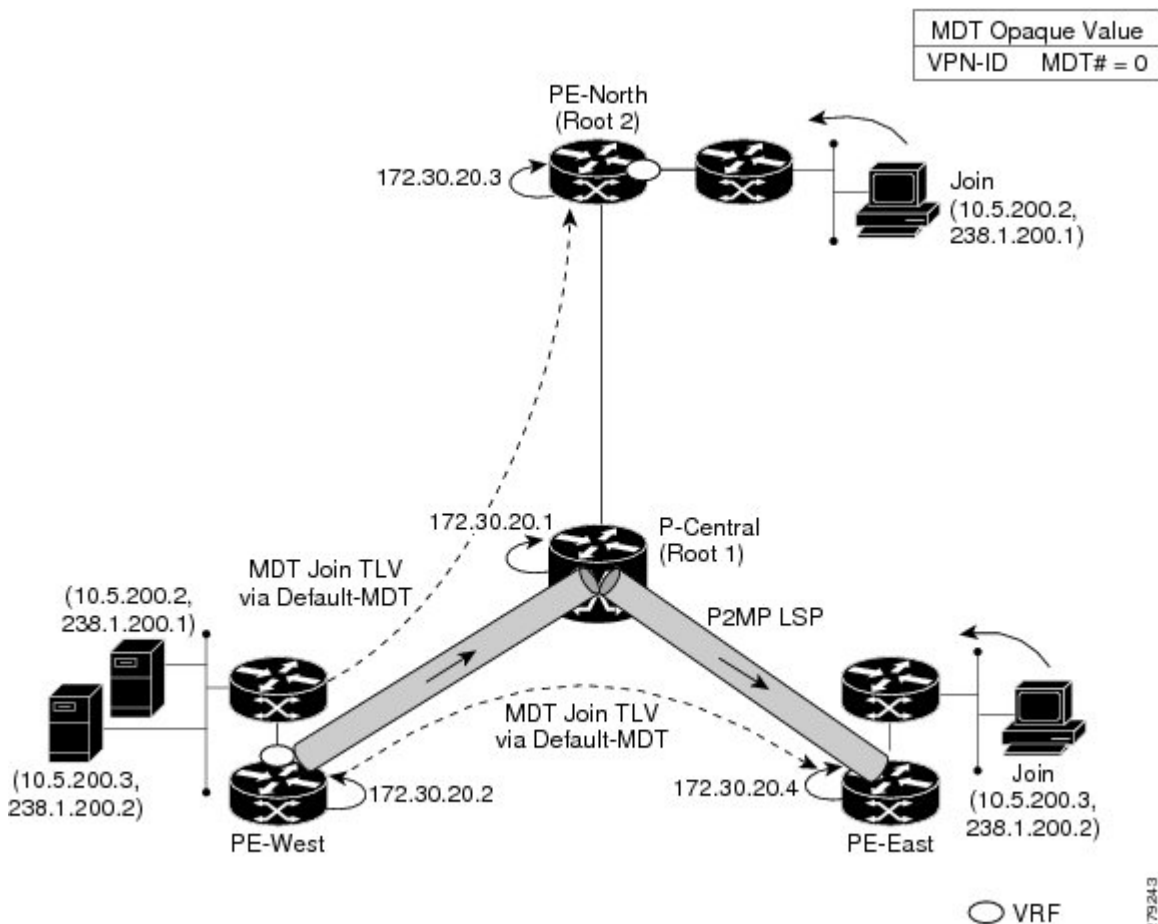
Central_P# show mpls mldp database opaque_type mdt 100:2
LSM ID      : E6000004
Uptime     : 00:42:03
Tree type  : MP2MP
FEC Root   : 172.30.20.3
Opaque length : 14 bytes
Opaque value : 07000B00 01000000 00020000 00009C
Opaque decoded : [mdt 100:2 0]
Upstream peer ID : 172.30.20.3:0, Label local (D): 104 remote (U): 313 active
Path Set ID : 48000003
Replication client(s):
172.30.20.2:0  uptime: 00:42:03  Path Set ID: CF000004
                 remote label (D): 207 local label (U): 115
                 nhop: 172.30.10.2 intrf: Serial4/0
172.30.20.4:0  uptime: 00:41:44  Path Set ID: 5800000E
                 remote label (D): 407 local label (U): 108
                 nhop: 172.30.10.10 intrf: Serial6/0
Central_P# show mpls forwarding-table | inc E6000004
104  207      mLDP:E6000004    251228     Se4/0      point2point
      407      mLDP:E6000004    251334     Se6/0      point2point
108  207      mLDP:E6000004     0          Se4/0      point2point
      313      mLDP:E6000004     0          Se5/0      point2point
115  313      mLDP:E6000004     0          Se5/0      point2point
      407      mLDP:E6000004     0          Se6/0      point2point

```

Data MDT Configuration

The following example shows how to configure the data MDT for an MLDP-based MVPN. This configuration is based on the sample topology illustrated in the figure.

Figure 11 Data MDT Example



The sample output in this section displays the data MDT configuration for all the PE devices. The **mdt data** commands are the only additional commands necessary. The first **mdt data** command allows a maximum of 60 data MDTs to be created, and the second **mdt data** command sets the threshold. If the number of data MDTs exceeds 60, then the data MDTs will be reused in the same way as they are for the mGRE tunnel method (the one with the lowest reference count).

```
ip pim vrf VRF mpls source Loopback0
!
ip vrf VRF
 rd 100:2
  vpn id 100:2
  route-target export 200:2
  route-target import 200:2
  mdt default mpls mldp 172.30.20.1 (P-Central)
  mdt default mpls mldp 172.30.20.3 (PE-North)
  mdt data mpls mldp 60
  mdt data threshold 1
```

- [VRF mroute Table--PE-West, page 23](#)
- [LSP-VIF Adjacencies--PE-West, page 23](#)

- [MLDP Database Entries, page 24](#)
- [LFIB Entry for the Data MDT, page 24](#)

VRF mroute Table--PE-West

The sample output in this section displays the VRF mroute table on PE-West before the high-bandwidth source exceeds the threshold. At this point there are two streams, representing each of the two VPN sources at PE-West, on a single MP2MP LSP (System ID D8000000). The LSP represents the default MDT accessed via LSP-VIF interface 0.

```
PE-West# show ip mroute vrf VRF verbose
.
.
(10.5.200.2, 238.1.200.1), 00:00:25/00:03:29, flags: sT
  Incoming interface: Serial6/0, RPF nbr 192.168.10.6
  Outgoing interface list:
    Lspvif0, LSM MDT: D8000000 (default),Forward/Sparse-Dense,
.
.
(10.5.200.3, 238.1.200.2), 00:11:14/00:02:48, flags: sT
  Incoming interface: Serial6/0, RPF nbr 192.168.10.6
  Outgoing interface list:
    Lspvif0, LSM MDT: D8000000 (default),Forward/Sparse-Dense,
.
.
```

The sample output in this section displays the output after the source transmission exceeds the threshold. PE-West sends an MDT Join TLV message to signal the creation of a data MDT. In this case, the data MDT number is 1, therefore PE-East will send a label mapping message back to PE-West with a FEC TLV containing root=PE-West, Opaque value=(mdt vpn-id 1). The System ID is now changed to 4E000003 signaling a different LSP; however, the LSP-VIF is still LSP-VIF interface 0. The (S, G) entry also has the “y” flag set indicating this stream has switched to a data MDT.

```
PE-West# show ip mroute vrf VRF 10.5.200.3 238.1.200.2 verbose
.
.
(10.5.200.3, 238.1.200.2), 00:00:08/00:03:27, flags: sTy
  Incoming interface: Serial6/0, RPF nbr 192.168.10.6
  MDT TX nr: 1 LSM-ID 4E000003
  Outgoing interface list:
    Lspvif0, LSM MDT: 4E000003 (data) Forward/Sparse-Dense,
```

LSP-VIF Adjacencies--PE-West

For the interface LSP-VIF, each virtual circuit represents a unique multipoint LSP forwarding instance. The correct adjacency is selected when sending the multicast packet. The sample output in this section displays the application of that concept on PE-West. There is a single LSP-VIF interface 0 interface, but it has three adjacencies as follows:

- 4E000003 is the single data MDT created for (10.5.200.3, 238.1.200.2)
- 58000000 is the default MDT (backup root)
- D8000000 is the default MDT (primary root)

```
PE-West# show adjacency lspvif 0

Protocol Interface Address
IP        Lspvif0  4E000003(5)
```

```

IP      Lspvif0          58000000(4)
IP      Lspvif0          D8000000(3)

```

MLDP Database Entries

The sample output in this section displays the MLDP entry for the data MDT (4E000003) on the ingress device PE-West. The following points about this entry should be noted:

- The tree type is P2MP with PE-West (172.30.20.2) as the root.
- The Opaque value is [mdt 100:2 1] denoting the first data MDT.
- There are no labels allocated as it is the root.
- There are two replication client entries on this tree.
- Label 112 will be used to send the traffic downstream towards PE-East (via P-Central).
- The MDT entry is an internal construct.

```

PE-West# show mpls mldp database id 4E000003
LSM ID : 4E000003 (RNR LSM ID: 8A000002)   Type: P2MP   Uptime : 00:04:54
FEC Root      : 172.30.20.2
Opaque decoded : [mdt 100:2 1]
Opaque length  : 11 bytes
Opaque value   : 07 000B 000001000000001000000000
RNR active LSP : (this entry)
Upstream client(s) : None
Replication client(s):
  MDT (VRF VRF)
    Uptime      : 00:04:54      Path Set ID   : 5000002
    Interface   : Lspvif0
172.30.20.1:0
  Uptime      : 01:41:43      Path Set ID   : D9000007
  Out label (D) : 27          Interface     : Serial4/0
  Local label (U) : 112       Next Hop      : 172.30.10.1

```

The sample output in this section displays the database entry for the data MDT on PE-East, the egress device. Also shown is the MDT Join TLV message that was sent from PE-West over the default MDT. The MDT Join TLV message contains all the necessary information to allow PE-East to create a label mapping message P2MP LSP back to the root of PE-West. Label 414 will be used by P-Central to send traffic to PE-East.

```
*Feb 19 04:43:24.039: PIM(1): MDT join TLV received for (10.5.200.3,238.1.200.2)
```

```
*Feb 19 04:43:24.039: MLDP: LDP root 172.30.20.2 added
```

```
*Feb 19 04:43:24.039: MLDP: [mdt 100:2 1] label mapping msg sent to 172.30.20.1:0
```

```

PE-East# show mpls mldp database opaque_type mdt 100:2 1
LSM ID : 4E000003 (RNR LSM ID: 8A000002)   Type: P2MP   Uptime : 00:04:54
FEC Root      : 172.30.20.2
Opaque decoded : [mdt 100:2 1]
Opaque length  : 11 bytes
Opaque value   : 07 000B 000001000000001000000000
RNR active LSP : (this entry)
Upstream client(s) : None
Replication client(s):
  MDT (VRF VRF)
    Uptime      : 00:04:54      Path Set ID   : 5000002
    Interface   : Lspvif0

```

LFIB Entry for the Data MDT

The sample output in this section displays the LFIB entry for the data MDT as it passes through P-Central and PE-East. The Tunnel ID used for the LSP is the Opaque value [mdt 100:2 1].

```
P-Central# show mpls for label 112
```

```

Local      Outgoing  Prefix      Bytes Label  Outgoing  Next Hop
Label      Label     or Tunnel Id  Switched     interface
111        414       [mdt 100:2 1] 2993584     Se6/0      point2point
PE-East# show mpls for label 400

Local      Outgoing  Prefix      Bytes Label  Outgoing  Next Hop
Label      Label     or Tunnel Id  Switched     interface
414 [T] No Label  [mdt 100:2 1][V] 3297312     aggregate/green

```

Example Migration from a PIM with mGRE-Based MVPN to an MLDP-Based MPVN

The following example shows an MLDP-based MVPN configuration that has been migrated from a PIM with mGRE based MVPN. The differences in the CLI from the PIM with mGRE-based MVPN are highlighted via comments below. In this example, MLDP derives the FEC from the import route target configured in the VRF.

```

ip vrf VRF
 rd 50:1111
  vpn id 50:10 ! MLDP-based MVPN configuration
  route-target export 100:100
  route-target import 100:100
  mdt preference mldp pim
  mdt default mpls mldp 1.1.1.1 ! MLDP-based MVPN configuration
  mdt default mpls mldp 2.2.2.2 ! MLDP-based MVPN configuration
  mdt data mpls mldp 255 ! MLDP-based MVPN configuration
  mdt data threshold 40 list 1 ! MLDP-based MVPN configuration
!
ip multicast-routing
ip multicast-routing vrf VRF
!
interface Loopback0
 ip address 205.1.0.1 255.255.255.0
 ip router isis
 ip pim sparse-dense-mode
!
interface Ethernet1/0
 ip vrf forwarding green
 ip address 220.0.2.1 255.255.255.0
 ip pim sparse-dense-mode
!
interface Ethernet2/0
 ip address 200.0.0.1 255.255.255.0
 ip pim sparse-dense-mode
 ip router isis
 mpls ip ! MLDP-based MVPN configuration
!
router isis
 net 49.0000.0000.0000.00

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP multicast commands	Cisco IOS Multicast Command Reference

Related Topic	Document Title
Overview of the IP multicast technology area	“ IP Multicast Technology Overview ” module
Concepts, tasks, and examples for configuring an IP multicast network using PIM	“ Configuring a Basic IP Multicast Network ” module

MIBs

MIB	MIBs Link
No new or modified MIBs are supported.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for MLDP-Based MVPN

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 **Feature Information for MLDP-Based MVPN**

Feature Name	Releases	Feature Information
MLDP-Based MVPN	15.0(1)S 15.1(1)SY Cisco IOS XE Release 3.8S	<p>The MLDP-based MVPN feature provides extensions to Label Distribution Protocol (LDP) for the setup of point-to-multipoint (P2MP) and multipoint-to-multipoint (MP2MP) label switched paths (LSPs) for transport in the Multicast Virtual Private Network (MVPN) core network.</p> <p>The following commands were introduced or modified: debug mpls mldp all, debug mpls mldp filter opaque type, debug mpls mldp generic, debug mpls mldp gr, debug mpls mldp mfi, debug mpls mldp mrrib, debug mpls mldp neighbor, debug mpls mldp packet, mdt data, mdt default, mdt preference, mpls mldp forwarding recursive, mpls logging notifications, mpls mldp path, show mpls mldp bindings, show mpls mldp count, show mpls mldp database, show mpls mldp label release, show mpls mldp neighbors, show mpls mldp root.</p>
IPV6 MVPN with MLDP	15.3(1)S Cisco IOS XE Release 3.8S	<p>Support was added for IPv6 addressing.</p> <p>The following commands were introduced or modified: mdt default, mdt data mpls mldp, mdt preference.</p>

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams,

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



MLDP Filtering

The MDLP Filtering feature adds filtering capabilities to the Cisco Multicast Label Distribution Protocol (MLDP) label-based Multicast Virtual Private Network (MVPN) solution.



Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.



Prerequisites for MLDP Filtering

- MDT must be configured.
- MLDP-based MVPN must be configured.



Information about MLDP Filtering

- [MLDP Filtering, page 35](#)
- [MLDP Disable on an Interface, page 35](#)

MLDP Filtering

MLDP Filtering prevents multicast traffic that is distributed to different sites via MVPNs from traveling on sections of the network by providing the following capabilities:

- Prevent MLDP traffic from traversing interconnections
- Map flows to MLDP data Multicast Distribution Tree (MDT) numbers
- Filter label mappings based on a particular range of MLDP tree numbers per VRF

The filtering feature uses FEC (Forward Equivalence Class) definitions to filter specified FECs on a per-peer basis. The list of peers for which a FEC is to be filtered is defined in an access control list (ACL). FEC-based filtering per peer is supported only for outbound filtering. If an MLDP stream is denied by the filter, then the router will not advertise label mappings to the filtered peer.

MLDP Filtering also enables you to filter label mappings based on a particular range of MLDP tree numbers per VRF. If a source and group (S,G) MVPN entry matches more than one data MDT configuration, all data MDT configurations are examined and the first configuration that contains an ACL that matches the (S,G) is picked. If none of the ACLs match the (S,G), then the tree number with the lowest ref_count among all the remaining no-ACL data MDT configurations is selected. If an (S,G) flow in the vrf is on a data MDT without an ACL and a new data MDT configuration with a matching ACL is configured, the (S,G) flow will not switch to the newly configured scope. The (S,G) flows which are already on the data MDT will switch only if the vrf mroutes are cleared.

Traffic can flow on the default MDT or it can be switched immediately to the data MDT after the (S,G) state is created on the ingress Provider Edge (PE) router. Immediate switch works for source specific-multicast (SSM) groups in the VRF only if the MDT data threshold is 0. As long as the (S,G) SSM state exists on the ingress PE router, traffic will stay on the data MDT.

MLDP Disable on an Interface

Multicast Label Distribution Protocol (MLDP) is automatically enabled on all interfaces on which Multiprotocol Label Switching (MPLS) dynamic label switching is enabled. Disabling MLDP on an interface prevents that interface from being used in path selection even if it is advertised as a path by route watch. If the only path returned by route watch is one on which MLDP is disabled, then the route to that peer or root is considered unreachable. If a router receives a label mapping on a particular interface on which MLDP is disabled, the router installs the label mapping and builds a tree upstream.

If there are two links to a given peer and one of them is MLDP-disabled, it is possible that the MPLS Forwarding Infrastructure (MFI) will use the disabled link for forwarding if recursive forwarding is configured. To ensure that the MLDP-disabled interface is not used by MFI, you must disable recursive forwarding.



How to Configure MLDP Filtering

- [Disabling MLDP on an Interface, page 37](#)
- [Filtering MLDP Traffic, page 38](#)
- [Mapping S and G Flows to MDT Trees, page 39](#)
- [Verifying MLDP Filtering, page 40](#)

Disabling MLDP on an Interface

MLDP is enabled by default on all MPLS-enabled interfaces. Perform this task to disable MDLP on the specified interface. We recommend that you disable MLDP on both sides of a link.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no mpls mldp**
5. **end**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2 configure terminal Example: Router# configure terminal	Enters global configuration mode.

Command or Action	Purpose
Step 3 <code>interface type number</code> Example: <pre>Router(config)# interface gigabitethernet 1/1</pre>	Enters interface configuration mode for configuring an interface.
Step 4 <code>no mpls mldp</code> Example: <pre>Router(config-if)# no mpls mldp</pre>	Disables MLDP on the interface being configured.
Step 5 <code>end</code> Example: <pre>Router(config-if)# end</pre>	Returns to privileged EXEC mode.

Filtering MLDP Traffic

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `mpls mldp fec fec_id opaque-type mdt vpn-id {vpn_id | any} scope {scope_id | any}`
4. `mpls mldp filter fec_id peer-list acl`
5. `exit`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: <pre>Router> enable</pre>	Enters privilege EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.

Command or Action	Purpose
<p>Step 3 <code>mpls mldp fec <i>fec_id</i> opaque-type mdt vpn-id {<i>vpn_id</i> any} scope {<i>scope_id</i> any}</code></p> <p>Example: <pre>Router(config-term)# mpls mldp fec 1 opaque-type mdt vpn-id any scope any</pre></p>	Defines an MLDP FEC. Repeat this step for each FEC to be defined.
<p>Step 4 <code>mpls mldp filter <i>fec_id</i> peer-list <i>acl</i></code></p> <p>Example: <pre>Router(config-term)# mpls mldp filter 1 peer-list 50</pre></p>	Filters out all MLDP trees that match the specified FEC definition to the peers in the specified peer-list standard ACL.
<p>Step 5 <code>exit</code></p> <p>Example: <pre>Router(config-term)# exit</pre></p>	Exits to privileged EXEC mode.

Mapping S and G Flows to MDT Trees

Extended access list (ACL) of range of (S,G) entries in VRF to be filtered must be configured.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `vrf definition vrf`
4. `mdt data mpls mldp num_tree [list acl] [scope scope_id] [immediate-switch]`
5. `end`

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example: <pre>PE> enable</pre></p>	<p>Enters privilege EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.

Command or Action	Purpose
Step 2 <code>configure terminal</code> Example: <pre>PE# configure terminal</pre>	Enters global configuration mode.
Step 3 <code>vrf definition vrf</code> Example: <pre>PE(config-term)# vrf definition blue</pre>	Configures a VRF address family and enters VRF address family configuration mode. Note You can use the <code>ip vrf</code> command to configure a VRF instance and enter VRF configuration mode.
Step 4 <code>mdt data mpls mldp num_tree [list acl] [scope scope_id] [immediate-switch]</code> Example: <pre>PE(config-vrf-af)# mdt data mpls mldp 100 peer-list 100 scope 1 immediate-switch</pre>	Configures MLDP data MDTs. Repeat this step for each data MDT to be configured.
Step 5 <code>end</code> Example: <pre>PE(config-vrf-af)# end</pre>	Returns to privileged EXEC mode.

Verifying MLDP Filtering

SUMMARY STEPS

1. `enable`
2. `show mpls mldp interface`
3. `show mpls mldp neighbors`
4. `show mpls mldp filter [fec-id]`
5. `show mpls mldp database`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: <pre>Router> enable</pre>	Enters privilege EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

Command or Action	Purpose
Step 2 <code>show mpls mldp interface</code> Example: <code>Router# show mpls mldp interface</code>	Displays whether MPLS and MLDP are enabled on the interfaces.
Step 3 <code>show mpls mldp neighbors</code> Example: <code>Router# show mpls mldp neighbors</code>	Displays the parameters by which a peer is filtered.
Step 4 <code>show mpls mldp filter [fec-id]</code> Example: <code>Router# show mpls mldp filter</code>	Displays information about filters and the peers associated with the filters.
Step 5 <code>show mpls mldp database</code> Example: <code>Router# show mpls mldp database</code>	Displays the MLDP paths label information for each MDT.



Configuration Examples for MLDP Filtering

- [Example: MLDP Filtering, page 43](#)
- [Example: S and G Mappings to Data MDT Tree Numbers, page 43](#)

Example: MLDP Filtering

The following example configuration shows the following:

- Peer P4 will be denied for all FECs (matches FEC 1).
- For FECs having VPN id 1:1 and any scope, peers P4 (matches FEC 1) and P2 (matches FEC 2) will be denied. Additionally peer P3 will be denied if FEC VPN id is 1:1 and scope 2 (matches FEC 4).
- For FECs having VPN id 2:2 and scope 1, peers P4 (matches FEC 1) and P2 (matches FEC 3) will be denied. Additionally peer P3 will be denied if FEC VPN id is 2:2 and scope 2 (matches FEC 4).
- For FECs having any VPN id and scope 2, peers P4 (matches FEC 1) and P3 (matches FEC 4) will be denied.
- Peer P4 will be denied for FEC with VPN id 3:3 and scope 3.

```
access-list 50 deny 4.4.4.4
access-list 50 permit any
access-list 51 deny 2.2.2.2
access-list 51 permit any
access-list 52 deny 3.3.3.3
access-list 52 permit any
.
.
.
mpls mldp fec 1 opaque-type mdt vpn-id any scope any
mpls mldp fec 2 opaque-type mdt vpn-id 1:1 scope any
mpls mldp fec 3 opaque-type mdt vpn-id 2:2 scope 1
mpls mldp fec 4 opaque-type mdt vpn-id all scope 2

mpls mldp filter 1 peer-list 50
mpls mldp filter 2 peer-list 51
mpls mldp filter 3 peer-list 51
mpls mldp filter 4 peer-list 52
```

Example: S and G Mappings to Data MDT Tree Numbers

This example shows the (S,G) mappings on the ingress PE for a given VRF (blue). Group range 232.1.1.0/24 is confined withing local scope 1 with traffic switching immediately to the data MDT. Group range 232.1.2.0/24 is confined to regional scope 2.

```
access-list 100 permit ip any 232.1.1.0 0.0.0.255
access-list 101 permit ip any 232.1.2.0 0.0.0.255
```

Example: S and G Mappings to Data MDT Tree Numbers

```
ip vrf blue
mdt data mpls mldp 100 list 100 scope 1 immediate-switch
mdt data mpls mldp 200 list 101 scope 2 immediate-switch
```



Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP Multicast commands	Cisco IOS IP Multicast Command Reference

Standards and RFCs

Standard/RFC	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html



Feature Information for MLDP Filtering

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2 Feature Information for MLDP Filtering

Feature Name	Releases	Feature Information
MLDP Filtering	15.1(3)S 15.1(1)SY	<p>The MDLP Filtering feature adds filtering capabilities to the Cisco Multicast Label Distribution Protocol (MLDP) label-based Multicast Virtual Private Network (MVPN) solution.</p> <p>The following commands were introduced or modified: mdt data mpls mldp, mpls mldp, mpls mldp fec, mpls mldp filter, show mpls mldp filter, show mpls mldp interface, show mpls mldp neighbors,</p>



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

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





HA Support for MLDP

The HA Support for MLDP feature enables Cisco Multicast Label Distribution Protocol (MLDP) to checkpoint sufficient signaling and forwarding information for repopulating the necessary database on a dual Route Processor (RP) platform on which Stateful Switchover/Nonstop Forwarding (SSO/NSF) and Label Distribution Protocol (LDP) Graceful Restart are configured, after a switchover.





Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.



Prerequisites for HA Support for MLDP

- Stateful Switchover/Nonstop Forwarding (SSO/NSF) and LDP Graceful Restart must be configured on the dual Route Processor (RP) platform.
- LDP Graceful Restart must be configured on the NSF router peers.
- The Cisco IOS release software installed on the active and standby RPs must support MLDP-based MVPN and HA Support for MLDP.



Restrictions for HA Support for MLDP

- If Label Distribution Protocol (LDP) Graceful Restart is not enabled on the dual Route Processor (RP) platform, Nonstop Forwarding (NSF) peers will remove existing forwarding and label information from their Multicast Label Distribution Protocol (MLDP) database entries immediately following a switchover.



Information About HA Support for MLDP

The HA Support for MLDP feature enables MLDP to checkpoint label forwarding or path set information. To support NSF, MLDP uses existing PIM HA architecture to checkpoint the information to the standby RP.

MDT data group creation is a dynamic event triggered by traffic exceeding a specified threshold. When the threshold is exceeded (requiring an MDT data group to be created) or when traffic falls below the threshold (requiring the MDT data group to be deleted), the router detecting the event creates, deletes, or updates an MDT data "send" entry, creates the corresponding (S,G) state, if necessary, and sends a message to PE peers to create, delete, or update a corresponding MDT data "receive" entry and the corresponding (S,G) state.

The active RP will checkpoint the current state of the MLDP peer, paths to peers, root, paths to root, and the database and replication/branch entry onto the standby RP and use this state to recreate the MLDP state after a switchover.



How to Monitor HA Support for MLDP

- [Displaying Check Pointed Information](#), page 61
- [Displaying Data MDT Mappings for MLDP on Standby Device](#), page 62

Displaying Check Pointed Information

SUMMARY STEPS

1. enable
2. show mpls mldp ha database
3. show mpls mldp ha database summary
4. show mpls mldp ha neighbor
5. show mpls mldp ha root
6. show mpls mldp ha count

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: PE2> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	show mpls mldp ha database Example: PE2# show mpls mldp ha database	Displays checkpoint data information.
Step 3	show mpls mldp ha database summary Example: PE2# show mpls mldp ha database summary	Displays synched database information only.

	Command or Action	Purpose
Step 4	show mpls mldp ha neighbor Example: PE2# show mpls mldp ha neighbor	Displays information about synched peers.
Step 5	show mpls mldp ha root Example: PE2# show mpls mldp ha root	Displays synched root information.
Step 6	show mpls mldp ha count Example: PE2# show mpls mldp ha count	Displays number of trees.

Displaying Data MDT Mappings for MLDP on Standby Device

SUMMARY STEPS

1. enable
2. show ip pim vrf *vrf* mdt send
3. show ip pim vrf *vrf* mdt recv

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: PE1-standby> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show ip pim vrf <i>vrf</i> mdt send Example: PE1-standby# show ip pim vrf blue mdt send	Displays data MDT mappings for MLDP.

Command or Action	Purpose
Step 3 <code>show ip pim vrf <i>vrf</i> mdt recv</code> Example: <code>PE1-standby# show ip pim vrf blue mdt recv</code>	Displays data MDT mappings for MLDP.



Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP Multicast commands	Cisco IOS IP Multicast Command Reference
Cisco HA	<i>High Availability Configuration Guide</i>

Standards and RFCs

Standard/RFC	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

MIBs

MIB	MIBs Link
--	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html



Feature Information for HA Support for MLDP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3 Feature Information for HA Support for MLDP

Feature Name	Releases	Feature Information
HA Support for MLDP	15.1(3)S 15.1(1)SY Cisco IOS XE Release 3.8S	<p>The HA Support for MLDP feature enables Cisco Multicast Label Distribution Protocol (MLDP) to checkpoint sufficient signaling and forwarding information for repopulating the necessary database on a dual Route Processor (RP) platform on which Stateful Switchover/ Nonstop Forwarding (SSO/ NSF) and Label Distribution Protocol (LDP) Graceful Restart are configured, after a switchover.</p> <p>The following commands were introduced or modified: show ip pim mdt recv, show ip pim mdt send, show mpls mldp ha database, show mpls mldp ha neighbor, show mpls mldp ha root.</p>



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

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





IPv6 Multicast Listener Discovery Protocol

- [Finding Feature Information, page 71](#)
- [Information About IPv6 Multicast Listener Discovery Protocol, page 71](#)
- [How to Configure IPv6 Multicast Listener Discovery Protocol, page 74](#)
- [Configuration Examples for IPv6 Multicast Listener Discovery Protocol, page 79](#)
- [Additional References, page 81](#)
- [IPv6 Multicast Listener Discovery Protocol, page 82](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 Multicast Listener Discovery Protocol

- [IPv6 Multicast Overview, page 71](#)
- [IPv6 Multicast Routing Implementation, page 72](#)
- [Multicast Listener Discovery Protocol for IPv6, page 73](#)
- [MLD Access Group, page 74](#)

IPv6 Multicast Overview

An IPv6 multicast group is an arbitrary group of receivers that want to receive a particular data stream. This group has no physical or geographical boundaries--receivers can be located anywhere on the Internet or in any private network. Receivers that are interested in receiving data flowing to a particular group must join the group by signaling their local device. This signaling is achieved with the MLD protocol.

Devices use the MLD protocol to learn whether members of a group are present on their directly attached subnets. Hosts join multicast groups by sending MLD report messages. The network then delivers data to a potentially unlimited number of receivers, using only one copy of the multicast data on each subnet. IPv6 hosts that wish to receive the traffic are known as group members.

Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best-effort reliability, just like IPv6 unicast packets.

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

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

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

How active a multicast group is, its duration, and its membership can vary from group to group and from time to time. A group that has members may have no activity.

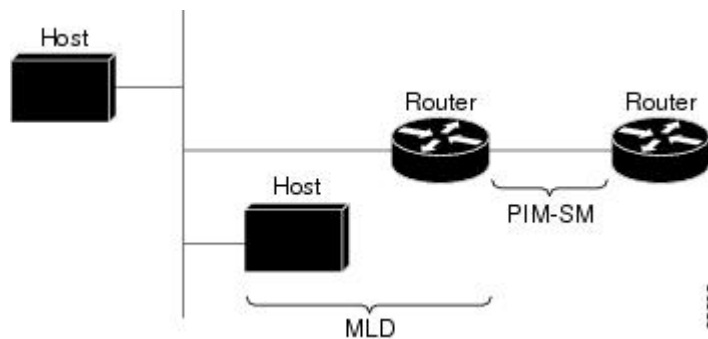
IPv6 Multicast Routing Implementation

Cisco software supports the following protocols to implement IPv6 multicast routing:

- MLD is used by IPv6 devices to discover multicast listeners (nodes that want to receive multicast packets destined for specific multicast addresses) on directly attached links. There are two versions of MLD:
 - MLD version 1 is based on version 2 of the Internet Group Management Protocol (IGMP) for IPv4.
 - MLD version 2 is based on version 3 of the IGMP for IPv4.
- IPv6 multicast for Cisco software uses both MLD version 2 and MLD version 1. MLD version 2 is fully backward-compatible with MLD version 1 (described in RFC 2710). Hosts that support only MLD version 1 will interoperate with a device running MLD version 2. Mixed LANs with both MLD version 1 and MLD version 2 hosts are likewise supported.
- PIM-SM is used between devices so that they can track which multicast packets to forward to each other and to their directly connected LANs.
- PIM in Source Specific Multicast (PIM-SSM) is similar to PIM-SM with the additional ability to report interest in receiving packets from specific source addresses (or from all but the specific source addresses) to an IP multicast address.

The figure below shows where MLD and PIM-SM operate within the IPv6 multicast environment.

Figure 12 IPv6 Multicast Routing Protocols Supported for IPv6



Multicast Listener Discovery Protocol for IPv6

To start implementing multicasting in the campus network, users must first define who receives the multicast. The MLD protocol is used by IPv6 devices to discover the presence of multicast listeners (for example, nodes that want to receive multicast packets) on their directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes. It is used for discovering local group and source-specific group membership. The MLD protocol provides a means to automatically control and limit the flow of multicast traffic throughout your network with the use of special multicast queriers and hosts.

The difference between multicast queriers and hosts is as follows:

- A querier is a network device, such as a device, that sends query messages to discover which network devices are members of a given multicast group.
- A host is a receiver, including devices, that send report messages to inform the querier of a host membership.

A set of queriers and hosts that receive multicast data streams from the same source is called a multicast group. Queriers and hosts use MLD reports to join and leave multicast groups and to begin receiving group traffic.

MLD uses the Internet Control Message Protocol (ICMP) to carry its messages. All MLD messages are link-local with a hop limit of 1, and they all have the alert option set. The alert option implies an implementation of the hop-by-hop option header.

MLD has three types of messages:

- Query--General, group-specific, and multicast-address-specific. In a query message, the multicast address field is set to 0 when MLD sends a general query. The general query learns which multicast addresses have listeners on an attached link.

Group-specific and multicast-address-specific queries are the same. A group address is a multicast address.

- Report--In a report message, the multicast address field is that of the specific IPv6 multicast address to which the sender is listening.
- Done--In a done message, the multicast address field is that of the specific IPv6 multicast address to which the source of the MLD message is no longer listening.

An MLD report must be sent with a valid IPv6 link-local source address, or the unspecified address (::), if the sending interface has not yet acquired a valid link-local address. Sending reports with the unspecified address is allowed to support the use of IPv6 multicast in the Neighbor Discovery Protocol.

For stateless autoconfiguration, a node is required to join several IPv6 multicast groups in order to perform duplicate address detection (DAD). Prior to DAD, the only address the reporting node has for the sending interface is a tentative one, which cannot be used for communication. Therefore, the unspecified address must be used.

MLD states that result from MLD version 2 or MLD version 1 membership reports can be limited globally or by interface. The MLD group limits feature provides protection against denial of service (DoS) attacks caused by MLD packets. Membership reports in excess of the configured limits will not be entered in the MLD cache, and traffic for those excess membership reports will not be forwarded.

MLD provides support for source filtering. Source filtering allows a node to report interest in listening to packets only from specific source addresses (as required to support SSM), or from all addresses except specific source addresses sent to a particular multicast address.

When a host using MLD version 1 sends a leave message, the device needs to send query messages to reconfirm that this host was the last MLD version 1 host joined to the group before it can stop forwarding

traffic. This function takes about 2 seconds. This "leave latency" is also present in IGMP version 2 for IPv4 multicast.

MLD Access Group

MLD access groups provide receiver access control in Cisco IPv6 multicast devices. This feature limits the list of groups a receiver can join, and it allows or denies sources used to join SSM channels.

How to Configure IPv6 Multicast Listener Discovery Protocol

- [Enabling IPv6 Multicast Routing, page 74](#)
- [Customizing and Verifying MLD on an Interface, page 75](#)
- [Disabling MLD Device-Side Processing, page 77](#)
- [Resetting the MLD Traffic Counters, page 78](#)
- [Clearing the MLD Interface Counters, page 79](#)

Enabling IPv6 Multicast Routing

IPv6 multicast uses MLD version 2. This version of MLD is fully backward-compatible with MLD version 1 (described in *RFC 2710*). Hosts that support only MLD version 1 will interoperate with a device running MLD version 2. Mixed LANs with both MLD version 1 and MLD version 2 hosts are likewise supported.

You must first enable IPv6 unicast routing on all interfaces of the device on which you want to enable IPv6 multicast routing .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 multicast-routing [vrf vrf-name]**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.

Command or Action	Purpose
Step 3 <code>ipv6 multicast-routing [vrf vrf-name]</code> Example: Device(config)# <code>ipv6 multicast-routing</code>	Enables multicast routing on all IPv6-enabled interfaces and enables multicast forwarding for PIM and MLD on all enabled interfaces of the device. <ul style="list-style-type: none"> IPv6 multicast routing is disabled by default when IPv6 unicast routing is enabled. On certain devices, the IPv6 multicast routing must also be enabled in order to use IPv6 unicast routing.

Customizing and Verifying MLD on an Interface

SUMMARY STEPS

- enable
- configure terminal
- interface *type number*
- ipv6 mld join-group [*group-address*] [[include | exclude] {*source-address* | source-list [*acl*]}]
- ipv6 mld access-group *access-list-name*
- ipv6 mld static-group [*group-address*] [[include| exclude] {*source-address* | source-list [*acl*]}]
- ipv6 mld query-max-response-time *seconds*
- ipv6 mld query-timeout *seconds*
- ipv6 mld query-interval *seconds*
- end
- show ipv6 mld groups [link-local] [*group-name* | *group-address*] [*interface-type* *interface-number*] [detail | explicit]
- show ipv6 mrib summary
- show ipv6 mld interface [*type number*]

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: Device# <code>configure terminal</code>	Enters global configuration mode.

Command or Action	Purpose
<p>Step 3 <code>interface type number</code></p> <p>Example:</p> <pre>Device(config)# interface GigabitEthernet 1/0/0</pre>	<p>Specifies an interface type and number, and places the device in interface configuration mode.</p>
<p>Step 4 <code>ipv6 mld join-group [group-address] [[include exclude] {source-address source-list [acl]}</code></p> <p>Example:</p> <pre>Device(config-if)# ipv6 mld join-group FF04::12 exclude 2001:DB8::10::11</pre>	<p>Configures MLD reporting for a specified group and source.</p>
<p>Step 5 <code>ipv6 mld access-group access-list-name</code></p> <p>Example:</p> <pre>Device(config-if)# ipv6 access-list acc-grp-1</pre>	<p>Allows the user to perform IPv6 multicast receiver access control.</p>
<p>Step 6 <code>ipv6 mld static-group [group-address] [[include exclude] {source-address source-list [acl]}</code></p> <p>Example:</p> <pre>Device(config-if)# ipv6 mld static-group ff04::10 include 100::1</pre>	<p>Statically forwards traffic for the multicast group onto a specified interface and cause the interface to behave as if a MLD joiner were present on the interface.</p>
<p>Step 7 <code>ipv6 mld query-max-response-time seconds</code></p> <p>Example:</p> <pre>Device(config-if)# ipv6 mld query-max-response- time 20</pre>	<p>Configures the maximum response time advertised in MLD queries.</p>
<p>Step 8 <code>ipv6 mld query-timeout seconds</code></p> <p>Example:</p> <pre>Device(config-if)# ipv6 mld query-timeout 130</pre>	<p>Configures the timeout value before the device takes over as the querier for the interface.</p>
<p>Step 9 <code>ipv6 mld query-interval seconds</code></p> <p>Example:</p> <pre>Device(config-if)# ipv6 mld query-interval 60</pre>	<p>Configures the frequency at which the Cisco IOS XE software sends MLD host-query messages.</p> <p>Caution Changing this value may severely impact multicast forwarding.</p>

Command or Action	Purpose
<p>Step 10 <code>end</code></p> <p>Example:</p> <pre>Device(config-if)# end</pre>	Exits to privileged EXEC mode.
<p>Step 11 <code>show ipv6 mld groups [link-local] [group-name group-address] [interface-type interface-number] [detail explicit]</code></p> <p>Example:</p> <pre>Device# show ipv6 mld groups GigabitEthernet 2/1/0</pre>	Displays the multicast groups that are directly connected to the device and that were learned through MLD.
<p>Step 12 <code>show ipv6 mfib summary</code></p> <p>Example:</p> <pre>Device# show ipv6 mfib summary</pre>	Displays summary information about the number of IPv6 Multicast Forwarding Information Base (MFIB) entries (including link-local groups) and interfaces.
<p>Step 13 <code>show ipv6 mld interface [type number]</code></p> <p>Example:</p> <pre>Device# show ipv6 mld interface GigabitEthernet 2/1/0</pre>	Displays multicast-related information about an interface.

Disabling MLD Device-Side Processing

A user might only want specified interfaces to perform IPv6 multicast and will therefore want to turn off MLD device-side processing on a specified interface.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `no ipv6 mld router`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3 <code>interface type number</code> Example: Device(config)# <code>interface GigabitEthernet 1/0/0</code>	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4 <code>no ipv6 mld router</code> Example: Device(config-if)# <code>no ipv6 mld router</code>	Disables MLD device-side processing on a specified interface.

Resetting the MLD Traffic Counters

SUMMARY STEPS

- `enable`
- `clear ipv6 mld [vrf vrf-name] traffic`
- `show ipv6 mld [vrf vrf-name] traffic`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.

	Command or Action	Purpose
Step 2	clear ipv6 mld [vrf vrf-name] traffic Example: Device# clear ipv6 mld traffic	Resets all MLD traffic counters.
Step 3	show ipv6 mld [vrf vrf-name] traffic Example: Device# show ipv6 mld traffic	Displays the MLD traffic counters.

Clearing the MLD Interface Counters

SUMMARY STEPS

1. enable
2. clear ipv6 mld [**vrf vrf-name**] counters *interface-type*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	clear ipv6 mld [vrf vrf-name] counters <i>interface-type</i> Example: Device# clear ipv6 mld counters GigabitEthernet1/0/0	Clears the MLD interface counters.

Configuration Examples for IPv6 Multicast Listener Discovery Protocol

- [Example: Enabling IPv6 Multicast Routing, page 80](#)
- [Example: Configuring the MLD Protocol, page 80](#)
- [Example: Disabling MLD Router-Side Processing, page 81](#)

Example: Enabling IPv6 Multicast Routing

The following example enables multicast routing on all interfaces and also enables multicast forwarding for PIM and MLD on all enabled interfaces of the device.

```
Device> enable
Device# configure terminal
Device(config)# ipv6 multicast-routing
```

Example: Configuring the MLD Protocol

The following example shows how to configure the query maximum response time, the query timeout, and the query interval on GigabitEthernet interface 1/0/0:

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/0

Device(config-if)# ipv6 mld query-max-response-time 20

Device(config-if)# ipv6 mld query-timeout 130

Device(config-if)# ipv6 mld query-interval 60
```

The following example shows how to configure MLD reporting for a specified group and source, allows the user to perform IPv6 multicast receiver access control, and statically forwards traffic for the multicast group onto GigabitEthernet interface 1/0/0:

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/0
Device(config)# ipv6 mld join-group FF04::10
Device(config)# ipv6 mld static-group FF04::10 100::1
Device(config)# ipv6 mld access-group acc-grp-1
```

The following example shows information from the **show ipv6 mld interface** command for GigabitEthernet interface 2/1/0:

```
Device# show ipv6 mld interface GigabitEthernet 2/1/1

GigabitEthernet2/1/1 is up, line protocol is up
Internet address is FE80::205:5FFF:FEAF:2C39/10
MLD is enabled in interface
Current MLD version is 2
MLD query interval is 125 seconds
MLD querier timeout is 255 seconds
MLD max query response time is 10 seconds
Last member query response interval is 1 seconds
MLD activity: 25 joins, 17 leaves
MLD querying router is FE80::205:5FFF:FEAF:2C39 (this system)
```

The following example displays the MLD protocol messages received and sent:

```
Device# show ipv6 mld traffic

MLD Traffic Counters
Elapsed time since counters cleared:00:00:21

Valid MLD Packets          Received      Sent
Queries                    1             0
Reports                    2             1
```

```

Leaves                0          0
Mtrace packets        0          0

Errors:
Malformed Packets    0
Bad Checksums        0
Martian source        0
Packets Received on MLD-disabled Interface 0

```

Example: Disabling MLD Router-Side Processing

The following example turns off MLD device-side processing on GigabitEthernet interface 1/0/0:

```

Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/0

```

```

Device(config-if)# no ipv6 mld router

```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
Cisco IOS commands	<i>Cisco IOS Master Commands List, All Releases</i>
IP multicast commands	<i>Cisco IOS IP Multicast Command Reference</i>
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	<i>Cisco IOS IPv6 Feature Mapping</i>

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

IPv6 Multicast Listener Discovery Protocol

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4 Feature Information for IPv6 Multicast Listener Discovery Protocol

Feature Name	Releases	Feature Information
IPv6 Multicast: Multicast Listener Discovery (MLD) Protocol, Versions 1 and 2	12.0(26)S	MLD is used by IPv6 routers to discover multicast listeners (nodes that want to receive multicast packets destined for specific multicast addresses) on directly attached links. The following commands were introduced or modified: debug ipv6 mld , ipv6 mld join-group , ipv6 mld static-group , ipv6 mld query-interval , ipv6 mld query-max-response-time , ipv6 mld query-timeout , ipv6 mld router , show ipv6 mld groups , show ipv6 mld groups summary , show ipv6 mld interface .
	12.2(18)S	
	12.2(25)SG	
	12.2(33)SRA	
	12.3(2)T	
	15.0(1)S	
	Cisco IOS XE Release 2.1	

Feature Name	Releases	Feature Information
IPv6 Multicast: MLD Access Group	12.2(33)SRE	The MLD access group provides receiver access control in Cisco IPv6 multicast routers. The following command was introduced: ipv6 mld access-group .
	12.2(50)SY	
	12.4(2)T	
	15.0(1)S	
	Cisco IOS XE Release 2.1	

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

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



MLD Group Limits

The IPv6 Multicast Listener Discovery (MLD) group limits feature provides global and per-interface MLD join limits.

- [Finding Feature Information, page 85](#)
- [Information About MLD Group Limits, page 85](#)
- [How to Implement MLD Group Limits, page 86](#)
- [Configuration Examples for MLD Group Limits, page 88](#)
- [Additional References, page 89](#)
- [Feature Information for MLD Group Limits, page 90](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About MLD Group Limits

- [Multicast Listener Discovery Protocol for IPv6, page 85](#)

Multicast Listener Discovery Protocol for IPv6

To start implementing multicasting in the campus network, users must first define who receives the multicast. The MLD protocol is used by IPv6 devices to discover the presence of multicast listeners (for example, nodes that want to receive multicast packets) on their directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes. It is used for discovering local group and source-specific group membership. The MLD protocol provides a means to automatically control and limit the flow of multicast traffic throughout your network with the use of special multicast queriers and hosts.

The difference between multicast queriers and hosts is as follows:

- A querier is a network device, such as a device, that sends query messages to discover which network devices are members of a given multicast group.

- A host is a receiver, including devices, that send report messages to inform the querier of a host membership.

A set of queriers and hosts that receive multicast data streams from the same source is called a multicast group. Queriers and hosts use MLD reports to join and leave multicast groups and to begin receiving group traffic.

MLD uses the Internet Control Message Protocol (ICMP) to carry its messages. All MLD messages are link-local with a hop limit of 1, and they all have the alert option set. The alert option implies an implementation of the hop-by-hop option header.

MLD has three types of messages:

- Query--General, group-specific, and multicast-address-specific. In a query message, the multicast address field is set to 0 when MLD sends a general query. The general query learns which multicast addresses have listeners on an attached link.

Group-specific and multicast-address-specific queries are the same. A group address is a multicast address.

- Report--In a report message, the multicast address field is that of the specific IPv6 multicast address to which the sender is listening.
- Done--In a done message, the multicast address field is that of the specific IPv6 multicast address to which the source of the MLD message is no longer listening.

An MLD report must be sent with a valid IPv6 link-local source address, or the unspecified address (::), if the sending interface has not yet acquired a valid link-local address. Sending reports with the unspecified address is allowed to support the use of IPv6 multicast in the Neighbor Discovery Protocol.

For stateless autoconfiguration, a node is required to join several IPv6 multicast groups in order to perform duplicate address detection (DAD). Prior to DAD, the only address the reporting node has for the sending interface is a tentative one, which cannot be used for communication. Therefore, the unspecified address must be used.

MLD states that result from MLD version 2 or MLD version 1 membership reports can be limited globally or by interface. The MLD group limits feature provides protection against denial of service (DoS) attacks caused by MLD packets. Membership reports in excess of the configured limits will not be entered in the MLD cache, and traffic for those excess membership reports will not be forwarded.

MLD provides support for source filtering. Source filtering allows a node to report interest in listening to packets only from specific source addresses (as required to support SSM), or from all addresses except specific source addresses sent to a particular multicast address.

When a host using MLD version 1 sends a leave message, the device needs to send query messages to reconfirm that this host was the last MLD version 1 host joined to the group before it can stop forwarding traffic. This function takes about 2 seconds. This "leave latency" is also present in IGMP version 2 for IPv4 multicast.

How to Implement MLD Group Limits

- [Implementing MLD Group Limits Globally, page 87](#)
- [Implementing MLD Group Limits per Interface, page 87](#)

Implementing MLD Group Limits Globally

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 mld [vrf *vrf-name*] state-limit *number***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ipv6 mld [vrf <i>vrf-name</i>] state-limit <i>number</i> Example: Device(config)# ipv6 mld state-limit 300	Limits the number of MLD states globally.

Implementing MLD Group Limits per Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *type number***
4. **ipv6 mld limit *number* [except *access-list*]**

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
<p>Step 2 <code>configure terminal</code></p> <p>Example:</p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 <code>interface type number</code></p> <p>Example:</p> <pre>Device(config)# interface FastEthernet 1/0</pre>	<p>Specifies an interface type and number, and places the device in interface configuration mode.</p>
<p>Step 4 <code>ipv6 mld limit number [except access-list]</code></p> <p>Example:</p> <pre>device(config-if)# ipv6 mld limit 100</pre>	<p>Limits the number of MLD states on a per-interface basis.</p>

Configuration Examples for MLD Group Limits

- [Example: Implementing MLD Group Limits, page 88](#)

Example: Implementing MLD Group Limits

This example shows the groups and channels that are being accounted when the MLD group limit function is active:

```
Device# show ipv6 mld groups FF03::1 detail
```

```
Interface:    FastEthernet5/1
Group:        FF03::1
Uptime:       00:00:05
Router mode:  EXCLUDE (Expires: 00:04:14)
Host mode:    INCLUDE
Last reporter: FE80::20A:8BFF:FE4D:6039
State accounted
Source list is empty
```

```
Interface:    FastEthernet5/1
Group:        FF33::1
Uptime:       00:00:03
Router mode:  INCLUDE
```

```

Host mode:      INCLUDE
Last reporter:  FE80::20A:8BFF:FE4D:6039
Group source list:
Source Address          Uptime    Expires    Fwd  Flags
2001:DB8:0::1          00:00:03  00:04:16  Yes  Remote Ac 4

```

The following example shows all of the groups joined by Fast Ethernet interface 2/1, including link-local groups used by network protocols.

```
Device# show ipv6 mld groups FastEthernet 2/1
```

```

MLD Connected Group Membership
Group Address      Interface          Uptime    Expires
FF02::2            FastEthernet2/1   3d18h    never
FF02::D            FastEthernet2/1   3d18h    never
FF02::16           FastEthernet2/1   3d18h    never
FF02::1:FF00:1     FastEthernet2/1   3d18h    00:00:27
FF02::1:FF00:79    FastEthernet2/1   3d18h    never
FF02::1:FF23:83C2  FastEthernet2/1   3d18h    00:00:22
FF02::1:FFAF:2C39  FastEthernet2/1   3d18h    never
FF06:7777::1      FastEthernet2/1   3d18h    00:00:26

```

The following is sample output from the **show ipv6 mld groups summary** command:

```
Device# show ipv6 mld groups summary
```

```

MLD Route Summary
No. of (*,G) routes = 5
No. of (S,G) routes = 0

```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
Cisco IOS commands	<i>Cisco IOS Master Commands List, All Releases</i>
IP multicast commands	<i>Cisco IOS IP Multicast Command Reference</i>
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	<i>Cisco IOS IPv6 Feature Mapping</i>

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for MLD Group Limits

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5 Feature Information for MLD Group Limits

Feature Name	Releases	Feature Information
MLD Group Limits	12.2(33)SRE	The IPv6 MLD group limits feature provides global and per-interface MLD join limits. The following commands were introduced or modified: ipv6 mld limit , ipv6 mld state-limit .
	12.2(50)SY	
	12.4(2)T	
	15.0(1)S	
	15.0(1)SY	
	15.1(1)SY	
	Cisco IOS XE Release 2.6	

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

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



MLDP In-Band Signaling/Transit Mode

This module contains information for configuring Multicast Label Distribution Protocol (MLDP) in-band signaling to enable the MLDP core to create (S,G) or (*,G) state without using out-of-band signaling such as Border Gateway protocol (BGP) or Protocol Independent Multicast (PIM).

- [Finding Feature Information, page 93](#)
- [Restrictions for MLDP In-Band Signaling, page 93](#)
- [Information About MLDP In-Band Signaling/Transit Mode, page 93](#)
- [How to Configure MLDP In-Band Signaling/Transit Mode, page 94](#)
- [Additional References, page 95](#)
- [Configuration Examples for MLDP In-Band Signaling/Transit Mode, page 96](#)
- [Feature Information for MLDP In-Band Signaling/Transit Mode, page 102](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for MLDP In-Band Signaling

- MLDP in-band signaling supports SOURCE-SPECIFIC MULTICAST (SSM) multicast traffic only.
- MLDP in-band signaling is not supported in the same VRF for which Rosen Model MLDP-based MVPN or GRE-based MVPN is configured.

Information About MLDP In-Band Signaling/Transit Mode

- [MLDP In-Band Signaling/Transit Mode, page 93](#)

MLDP In-Band Signaling/Transit Mode

Multicast Label Distribution Protocol (MLDP)-supported multicast VPN (MVPN) allows VPN multicast streams to be aggregated over a VPN-specific tree. No customer state is created in the MLDP core; there is

only state for default and data multicast distribution trees (MDTs). In certain scenarios, the state created for VPN streams is limited and does not appear to be a risk or limiting factor. In these scenarios, MLDP can build in-band MDTs that are transit Label Switched Paths (LSPs).

Trees used in a VPN space are MDTs. Trees used in the global table are transit point-to-multipoint (P2MP) or multipoint-to-multipoint (MP2MP) LSPs. In both cases, a single multicast stream (VPN or not) is associated with a single LSP in the MPLS core. The stream information is encoded in the Forwarding Equivalence Class (FEC) of the LSP. This is in-band signaling.

MLDP in-band signaling uses access control lists (ACLs) with the range of the multicast (S, G) to be transported by the MLDP LSP. Each multicast channel (S, G) maps, one-to-one, to each tree in the in-band tree. The (S,G) join is registered in the Multicast Routing Information Base (MRIB), which is a client of MLDP. Each MLDP LSP is identified by the FEC of [(S,G) + RD], where RD is the Route Distinguisher (RD) obtained from BGP. This differs from MLDP-based MVPN, where the identity is in a FEC of [MDT #, VPN ID, Tree #].

The ingress Provider Edge (PE) device uses the FEC to decode the stream information and associate the multicast stream with the LSP (in the FEC). This service model is only applicable for transporting Protocol Independent Multicast (PIM) source-specific multicast (SSM) traffic. There is no need to run PIM over the LSP because the stream signaling is done in-band.

The MLDP In-Band Signaling/Transit Mode feature is supported on IPv4 and IPv6 networks. MLDP in-band signaling and MLDP-based MVPN cannot be supported in the same VRF.

How to Configure MLDP In-Band Signaling/Transit Mode

- [Enabling In-Band Signaling on a PE Device, page 94](#)

Enabling In-Band Signaling on a PE Device

- VRF instances for in-band signaling must be configured.
- Access control lists (ACLs) for controlling streams must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Use one of the following commands:
 - **ip multicast [vrf vrf] mpls mldp [range act]**
 - **ipv6 multicast [vrf vrf] mpls mldp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Device> enable	<ul style="list-style-type: none"> • Enter your password if prompted.

Command or Action	Purpose
<p>Step 2 <code>configure terminal</code></p> <p>Example: Device# <code>configure terminal</code></p>	Enters global configuration mode.
<p>Step 3 Use one of the following commands:</p> <ul style="list-style-type: none"> • <code>ip multicast [vrf vrf] mpls mldp [range acl]</code> • <code>ipv6 multicast [vrf vrf] mpls mldp</code> <p>Example: Device (config)# <code>ip multicast vrf vrf1 mpls mldp</code></p> <p>Device (config)# <code>ipv6 multicast vrf vrf1 mpls mldp</code></p>	<p>Brings up the MLDP MRIB process and registers MLDP with the MRIB.</p> <ul style="list-style-type: none"> • To enable in-band signaling globally, use this command without the <code>vrf vrf</code> keyword and argument combination. • IPv4 only: To identify streams for in-band signaling, use this command with the <code>range</code> keyword on the egress PE.

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
Cisco IOS commands	<i>Cisco IOS Master Commands List, All Releases</i>
IP multicast commands	<i>Cisco IOS IP Multicast Command Reference</i>
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	<i>Cisco IOS IPv6 Feature Mapping</i>

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Configuration Examples for MLDP In-Band Signaling/Transit Mode

- [Example: In-Band Signaling on PE1, page 96](#)
- [Example: In-Band Signaling on PE2, page 99](#)

Example: In-Band Signaling on PE1

```

PE1# show running-config
Building configuration...

Current configuration : 8247 bytes
!
! Last configuration change at 12:44:13 IST Thu Nov 15 2012
!

hostname PE1
!
mls ipv6 vrf
!
vrf definition vrf1
 rd 1:1
  vpn id 1:1
  route-target export 1:1
  route-target import 1:1
!
 address-family ipv4
  route-target export 1:1
  route-target import 1:1
  exit-address-family
!
 address-family ipv6

```

```

    route-target export 1:1
    route-target import 1:1
  exit-address-family
!

ip multicast-routing
ip multicast-routing vrf vrfl
ip multicast hardware-switching replication-mode egress
ip multicast mpls mldp
ip multicast vrf vrfl mpls mldp
!
!
!
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 multicast-routing vrf vrfl
ipv6 multicast rpf use-bgp
ipv6 multicast mpls source Loopback0
ipv6 multicast mpls mldp
ipv6 multicast vrf vrfl rpf use-bgp
ipv6 multicast vrf vrfl mpls source Loopback0
ipv6 multicast vrf vrfl mpls mldp
!
!
vtp domain cisco
vtp mode off
mpls label protocol ldp
mpls ldp graceful-restart
mls flow ip interface-full
no mls flow ipv6
mls rate-limit multicast ipv4 igmp 100 10
mls cef error action reset
mls mpls tunnel-recir
multilink bundle-name authenticated
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
no diagnostic bootup level
!
redundancy
  main-cpu
    auto-sync running-config
  mode sso
!

vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
interface Loopback0
  ip address 1.1.1.1 255.255.255.255
  ip pim sparse-mode
  ip ospf 100 area 0
  ipv6 address 1::1:1:1/64
  ipv6 enable
!
.
.
!
interface GigabitEthernet2/0/0.1
  encapsulation dot1Q 2
  vrf forwarding vrfl
  ip address 192.0.2.1 255.255.255.0
  ip pim sparse-mode
  ip igmp version 3
  ipv6 address FE80::10:1:1 link-local
  ipv6 address 2001:DB8::/64
  ipv6 enable
!
interface GigabitEthernet2/0/0.2000

```

```

encapsulation dot1Q 2000
ip address 192.0.2.2 255.255.255.0
ip pim sparse-mode
ip igmp version 3
ipv6 address 2001:DB8:0:1/64
ipv6 enable
!
.
.
.
interface GigabitEthernet2/0/12
ip address 192.0.2.3 255.255.255.0
ip pim sparse-mode
ip ospf 100 area 0
ipv6 address 2001:DB8::/64
ipv6 enable
mpls ip
mpls label protocol ldp
no mls qos trust
!
!
!
router ospf 100
router-id 1.1.1.1
!
router bgp 100
bgp log-neighbor-changes
neighbor 2.2.2.2 remote-as 100
neighbor 2.2.2.2 update-source Loopback0
neighbor 3.3.3.3 remote-as 100
neighbor 3.3.3.3 update-source Loopback0
neighbor 4.4.4.4 remote-as 100
neighbor 4.4.4.4 update-source Loopback0
!
address-family ipv4
redistribute static
redistribute connected
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-community both
neighbor 3.3.3.3 activate
neighbor 3.3.3.3 send-community both
neighbor 4.4.4.4 activate
neighbor 4.4.4.4 send-community both
exit-address-family
!
address-family vpnv4
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-community extended
neighbor 3.3.3.3 activate
neighbor 3.3.3.3 send-community extended
neighbor 4.4.4.4 activate
neighbor 4.4.4.4 send-community extended
exit-address-family
!
address-family ipv4 mdt
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-community extended
neighbor 3.3.3.3 activate
neighbor 3.3.3.3 send-community extended
neighbor 4.4.4.4 activate
neighbor 4.4.4.4 send-community extended
exit-address-family
!
address-family ipv6
redistribute connected
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-community extended
neighbor 2.2.2.2 send-label
neighbor 3.3.3.3 activate
neighbor 3.3.3.3 send-community extended
neighbor 3.3.3.3 send-label
neighbor 4.4.4.4 activate
neighbor 4.4.4.4 send-community extended

```



```

    neighbor 4.4.4.4 send-label
  exit-address-family
  !
  address-family vpnv6
    neighbor 2.2.2.2 activate
    neighbor 2.2.2.2 send-community extended
    neighbor 3.3.3.3 activate
    neighbor 3.3.3.3 send-community extended
    neighbor 4.4.4.4 activate
    neighbor 4.4.4.4 send-community extended
  exit-address-family
  !
  address-family ipv4 vrf vrf1
    redistribute connected
  exit-address-family
  !
  address-family ipv6 vrf vrf1
    redistribute connected
  exit-address-family
  !
no ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip pim ssm default
ip pim mpls source Loopback0
ip pim vrf vrf1 ssm default
ip pim vrf vrf1 mpls source Loopback0
ip route 192.0.2.25 255.255.255.255 7.37.0.1
!
!
mpls ldp router-id Loopback0 force
!
!
!
end

```

Example: In-Band Signaling on PE2

```

PE2# show running-config
Building configuration...

Current configuration : 7609 bytes
!
! Last configuration change at 13:18:45 IST Thu Nov 15 2012
!
hostname PE2
!
mls ipv6 vrf
!
vrf definition vrf1
  rd 1:1
  vpn id 1:1
  route-target export 1:1
  route-target import 1:1
  !
  address-family ipv4
    route-target export 1:1
    route-target import 1:1
  exit-address-family
  !
  address-family ipv6
    route-target export 1:1
    route-target import 1:1
  exit-address-family
!
.
.
.
!
ip multicast-routing
ip multicast-routing vrf vrf1

```

```

ip multicast hardware-switching replication-mode egress
ip multicast mpls mldp
ip multicast vrf vrfl mpls mldp
!
!
!
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 multicast-routing vrf vrfl
ipv6 multicast rpf use-bgp
ipv6 multicast mpls source Loopback0
ipv6 multicast mpls mldp
ipv6 multicast vrf vrfl rpf use-bgp
ipv6 multicast vrf vrfl mpls source Loopback0
ipv6 multicast vrf vrfl mpls mldp
!
!
vtp domain isbu-devtest
vtp mode off
mpls label protocol ldp
mpls ldp graceful-restart
mls flow ip interface-full
no mls flow ipv6
mls cef error action reset
multilink bundle-name authenticated
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
diagnostic bootup level minimal
!
redundancy
  main-cpu
  auto-sync running-config
  mode sso
!
!
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
 ip pim sparse-mode
 ip ospf 100 area 0
 ipv6 enable
!
.
.
.
!
interface GigabitEthernet3/0/3.1
 encapsulation dot1q 2
 vrf forwarding vrfl
 ip address 192.0.2.1 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 ipv6 address FE80::30:1:1 link-local
 ipv6 address 2001:DB8::/64
 ipv6 enable
!
interface GigabitEthernet3/0/3.2000
 encapsulation dot1q 2000
 ip address 192.0.2.2 255.255.255.0
 ip pim sparse-mode
 ip igmp static-group 232.1.1.1 source 50.0.0.2
 ip igmp version 3
 ipv6 address 2001:DB8:0:1/64
 ipv6 enable
!
.
.
.
!

```

```
interface GigabitEthernet4/15
 ip address 192.0.2.3 255.255.255.0
 ip pim sparse-mode
 ip ospf 100 area 0
 ipv6 address 2001:DB8::/64
 ipv6 enable
 mpls ip
 mpls label protocol ldp
!
.
.
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 100
 router-id 4.4.4.4
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback0
!
 address-family ipv4
  redistribute static
  redistribute connected
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
!
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
 exit-address-family
!
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
 exit-address-family
!
 address-family ipv6
  redistribute connected
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
  neighbor 1.1.1.1 send-label
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 2.2.2.2 send-label
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
  neighbor 3.3.3.3 send-label
 exit-address-family
!
 address-family vpnv6
  neighbor 1.1.1.1 activate
```

```

neighbor 1.1.1.1 send-community extended
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-community extended
neighbor 3.3.3.3 activate
neighbor 3.3.3.3 send-community extended
exit-address-family
!
address-family ipv4 vrf vrfl
  redistribute connected
exit-address-family
!
address-family ipv6 vrf vrfl
  redistribute connected
exit-address-family
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip pim ssm default
ip pim mpls source Loopback0
ip pim vrf vrfl ssm default
ip pim vrf vrfl mpls source Loopback0
ip route 192.0.2.25 255.255.255.255 7.37.0.1
!
!
mpls ldp router-id Loopback0 force
!
!
.
.
!
!
end

```

Feature Information for MLDP In-Band Signaling/Transit Mode

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 6 **Feature Information for MLDP In-Band Signaling/Transit Mode**

Feature Name	Releases	Feature Information
MLDP In-Band Signaling/Transit Mode	15.3(1)S Cisco IOS XE 3.8S	<p data-bbox="1154 344 1511 785">Multicast Label Distribution Protocol (MLDP) in-band signaling supports point-to-multipoint (P2P) and multipoint-to-multipoint (MP2MP) Label Switched Paths (LSPs) and enables the MLDP core to create (S,G) or (*,G) state without using out-of-band signaling such as Border Gateway Protocol (BGP) or Protocol Independent Multicast (PIM). This feature is supported for IPv4 and IPv6 multicast groups.</p> <p data-bbox="1154 806 1511 926">The following commands were introduced or modified: ip multicast mpls mldp, ipv6 multicast mpls mldp.</p>

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

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

