



Implementing Layer-3 Multicast Routing

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

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.

The following protocols are supported to implement multicast routing:

- IGMP—IGMP is used between hosts on a network (for example, LAN) and the routers on that network to track the multicast groups of which hosts are members.
- PIM SSM— Protocol Independent Multicast in Source-Specific Multicast (PIM-SSM) has the ability to report interest in receiving packets from specific source addresses (or from all but the specific source addresses), to an IP multicast address.

Prerequisites for Implementing Multicast Routing

- You must install and activate the multicast RPM package.
- You must be familiar with IPv4 multicast routing configuration tasks and concepts.
- Unicast routing must be operational.

Restrictions

- Multicast over access or core pseudowire is not supported.
- [Enabling Multicast, on page 2](#)
- [Supported Multicast Features, on page 3](#)
- [Restrictions for Multicast, on page 4](#)
- [Protocol Independent Multicast, on page 5](#)
- [PIM BFD Overview, on page 5](#)
- [Reverse Path Forwarding, on page 7](#)
- [RPF Vector Encoding Using IETF Standard, on page 8](#)
- [PIM Bootstrap Router, on page 8](#)
- [PIM-Source Specific Multicast, on page 10](#)

- Multicast Source Discovery Protocol, on page 14
- PIM-Sparse Mode, on page 19
- Designated Routers, on page 21
- Internet Group Management Protocol, on page 23
- IPv6 Multicast for Multiple Sources, on page 29
- Statistics for Ingress Multicast Routes, on page 29
- Multicast Route Statistics , on page 31
- Use Case: Video Streaming, on page 33
- Multicast over Access Pseudo-Wire, on page 34
- Multicast Label Distribution Protocol (MLDP) for Core, on page 39
- Multicast MLDP Profile 14 support on an Edge Router, on page 40
- Configuration Example for MLDP on Core, on page 41
- Label Switched Multicast (LSM) Multicast Label Distribution Protocol (mLDP) based Multicast VPN (mVPN) Support, on page 41
- Configure VRF MLDP In-Band Signaling on Edge Routers , on page 45
- Configure Global MLDP In-band Signaling on Edge Routers, on page 46
- Configuration Examples for MVPN Profiles, on page 46
- Configuration Examples for Inband mLDP Profiles on Edge Routers, on page 47
- Verification of MLDP Configuration on Edge Routers, on page 48

Enabling Multicast

Configuration Example

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

```
Router#config
Router (config) #multicast-routing
Router (config-mcast) #address-family ipv4
Router (config-mcast-default-ipv4) #interface all enable
*/In the above command, you can also indicate a specific interface (For example, interface
TenGigE0/11/0/0)
for enabling multicast only on that interface/*
Router (config-mcast-default-ipv4) #commit
```

Running Configuration

```
Router#show running multicast routing
multicast-routing
  address-family ipv4
  interface all enable
  !
```

Verification

Verify that the Interfaces are enabled for multicast.

```
Router#show mfib interface location 0/RP0/cpu0
Interface : FINT0/RP0/cpu0 (Enabled)
SW Mcast pkts in : 0, SW Mcast pkts out : 0
TTL Threshold : 0
Ref Count : 2
Interface : TenGigE0/11/0/0 (Enabled)
```

```
SW Mcast pkts in : 0, SW Mcast pkts out : 0
TTL Threshold : 0
Ref Count : 3
Interface : TenGigE0/11/0/1 (Enabled)
SW Mcast pkts in : 0, SW Mcast pkts out : 0
TTL Threshold : 0
Ref Count : 13
Interface : Bundle-Ether1 (Enabled)
SW Mcast pkts in : 0, SW Mcast pkts out : 0
TTL Threshold : 0
Ref Count : 4
Interface : Bundle-Ether1.1 (Enabled)
SW Mcast pkts in : 0, SW Mcast pkts out : 0
TTL Threshold : 0
```

Supported Multicast Features

- Hardware Offloaded BFD for PIMv4 is supported.
- IPv4 and IPV6 static groups for both IGMPv2/v3 and MLDv1/v2 are supported.
- SSM mapping is supported.
- PIMv4/v6 over Bundle sub-interface is supported.
- Loadbalancing for multicast traffic for ECMP links and bundles is supported.
- Router needs to be reloaded to recover, if TCAM space is exceeded.
- Multicast MAC and multicast IP address should be matched for both Layer 2 and Layer 3 traffic, else traffic may be dropped by ASIC. L2 flooding is not supported.
- Multicast traffic fragmentation in hardware is not supported .
- Multicast traffic without Spanning-Tree protocol is supported at Layer 2 for multicast traffic without snooping enabled.
- IPv6 multicast MLD joins are subjected to hop by hop LPTS punt policer. Tweaking this policer to a higher value achieves convergence at higher scale.

Also, adjust the ICMP control traffic LPTS hardware policer to a higher value for optimal convergence at higher scale.

IGMP Snooping Features

Supported Features

- IGMP Snooping on bridge domain is supported
- Multicast on BVI is supported.
- EVPN IGMP State Sync using IGMP snooping profile is supported.

Restrictions for Multicast

- Multicast over core pseudowire is not supported.
- Multicast over access or core pseudowire is not supported.
- Multicast over VRF-lite is not supported.
- MFIB stats S,G not supported.
- The hw-module profile mfib statistics is not supported.
- BVI based multicast is not supported.
- IGMP snooping is not supported.
- IGMP snooping over VPLS is not supported.
- MLDP is not supported on the edge role.
- IPv6 PIM SM is not supported.
- AutoRP for IPv4 PIM SM is not supported.
- Static IPv4 mroutes are not supported.
- Redundant sources for IPv6 PIM SSM is not supported. Multiple sources for the same group for IPv6 PIM SSM is not supported (S1,G.S2,G do not work).
- G.8032 or other L2 based redundancy and convergence protocols are not supported for multicast traffic.
- QoS over Multicast not supported.
- L2 Bundle for multicast is not supported.
- MVPN GRE is not supported.

Restrictions for IGMP Snooping

- BVI enabled with Layer3 multicast and IGMP snooping is disabled.
- Multicast Sparse mode is not supported for flows for flows for which igmp snooping is enabled in given BD/BVI.
- Any *, G report IGMPv2/IGMPv3(exclude null) does not work. Sending *, G reports also breaks existing flows.
- PIMv4 Hello on BVI is does not gett punted due to punt code issue. Inject is fine.
- Different type of encapsulations such as dot1ad and qinq do not work for L2 subinterface attachment circuit. Encapsulation untagged is not supprted.
- BVI shutdown breaks punt path. Query Packets do not get punted.
- Egress traffic tagged with wrong encapsulation is not supported for traffic incoming to the BVI interface.
- Flooding on bridge domian when there is a BVI with no snooping profile attached is not supported on the access or P-Edge routers.

- IPv6 Multicast on BVI or pure bridge domain is not supported.

Protocol Independent Multicast

Protocol Independent Multicast (PIM) is a multicast routing protocol used to create multicast distribution trees, which are used to forward multicast data packets.

Proper operation of multicast depends on knowing the unicast paths towards a source or an RP. PIM relies on unicast routing protocols to derive this reverse-path forwarding (RPF) information. As the name PIM implies, it functions independently of the unicast protocols being used. PIM relies on the Routing Information Base (RIB) for RPF information. Protocol Independent Multicast (PIM) is designed to send and receive multicast routing updates.

PIM on Bundle-Ethernet subinterface is supported.

PIM BFD Overview

The BFD Support for Multicast (PIM) feature, also known as PIM BFD, registers PIM as a client of BFD. PIM can then utilize BFD's fast adjacency failure detection. When PIM BFD is enabled, BFD enables faster failure detection without waiting for hello messages from PIM.

At PIMs request, as a BFD client, BFD establishes and maintains a session with an adjacent node for maintaining liveness and detecting forwarding path failure to the adjacent node. PIM hellos will continue to be exchanged between the neighbors even after BFD establishes and maintains a BFD session with the neighbor. The behavior of the PIM hello mechanism is not altered due to the introduction of this feature. Although PIM depends on the Interior Gateway Protocol (IGP) and BFD is supported in IGP, PIM BFD is independent of IGP's BFD.

Protocol Independent Multicast (PIM) uses a hello mechanism for discovering new PIM neighbors between adjacent nodes. The minimum failure detection time in PIM is 3 times the PIM Query-Interval. To enable faster failure detection, the rate at which a PIM hello message is transmitted on an interface is configurable. However, lower intervals increase the load on the protocol and can increase CPU and memory utilization and cause a system-wide negative impact on performance. Lower intervals can also cause PIM neighbors to expire frequently as the neighbor expiry can occur before the hello messages received from those neighbors are processed. When PIM BFD is enabled, BFD enables faster failure detection without waiting for hello messages from PIM.

Configure PIM BFD



Note PIM BFD for IPv6 is not supported.

This section describes how you can configure PIM BFD

```
Router# configure
Router(config)# router pim address-family ipv4
Router(config-pim-default-ipv4)# interface HundredGigE0/9/0/0
Router(config-pim-ipv4-if)# bfd minimum-interval 10
Router(config-pim-ipv4-if)# bfd fast-detect
Router(config-pim-ipv4-if)# bfd multiplier 3
```

```

Router(config-pim-ipv4)# exit
Router(config-pim-default-ipv4)# interface TenGigE0/11/0/0
Router(config-pim-ipv4-if)# bfd minimum-interval 50
Router(config-pim-ipv4-if)# bfd fast-detect
Router(config-pim-ipv4-if)# bfd multiplier 3
Router(config-pim-ipv4-if)# exit

```

Running Configuration

```

router pim
 address-family ipv4
   interface HundredGigE 0/9/0/0
     bfd minimum-interval 10
     bfd fast-detect
     bfd multiplier 3
   !
   interface TenGigE 0/11/0/0
     bfd minimum-interval 50
     bfd fast-detect
     bfd multiplier 3
   !
 !
 !
 !
 !
 !

```

Verification

The show outputs given in the following section display the details of the configuration of the PIM BFD, and the status of their configuration.

```

Router# show bfd session
Wed Nov 22 08:27:35.952 PST
Interface          Dest Addr      Local det time(int*mult)  State      Echo      Async
H/W              NPU
-----
Hu0/9/0/0         10.12.12.2     0s(0s*0) 90ms(30ms*3)           UP
0/RP0/CPU0
Te0/11/0/0        10.112.112.2  0s(0s*0) 90ms(30ms*3)           UP           Yes  0/RP0/CPU0

```

```

Router# show bfd client
Name              Node           Num sessions
-----
L2VPN_ATOM       0/RP0/CPU0    0
MPLS-TR          0/RP0/CPU0    0
bgp-default      0/RP0/CPU0    0
bundlemgr_distrib 0/RP0/CPU0   14
isis-1           0/RP0/CPU0    0

```

```

object_tracking 0/RP0/CPU0 0
pim6             0/RP0/CPU0 0
pim            0/RP0/CPU0 0
service-layer   0/RP0/CPU0 0

```

Reverse Path Forwarding

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

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

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

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

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

Setting the Reverse Path Forwarding Statically

Configuration Example

The following example configures the static RPF rule for IP address 10.0.0.1:

```

Router#configure
Router(config)#multicast-routing
Router(config-mcast)#address-family ipv4
Router(config-mcast)#static-rpf 10.0.0.1 32 TenGigE 0/0/0/1 192.168.0.2
Router(config-mcast)#commit

```

Running Configuration

```

multicast-routing
  address-family ipv4
    static-rpf 10.10.10.2 32 TenGigE0/0/0/1 192.168.0.2

```

Verification

Verify that RPF is chosen according to the static RPF configuration for 10.10.10.2

```

Router#show pim rpf
Table: IPv4-Unicast-default

```

```
* 10.10.10.2/32 [0/0]
  via GigabitEthernet0/0/0/1 with rpf neighbor 192.168.0.2
```

RPF Vector Encoding Using IETF Standard

RPF vector is a PIM proxy that lets core routers without RPF information forward join and prune messages for external sources (for example, a MPLS-based BGP-free core, where the MPLS core router is without external routes learned from BGP). The RPF vector encoding is now compatible with the new IETF encoding. The new IETF standard encodes PIM messages using PIM Hello option 26.

Configuring RPF Vector (IETF Standard Encoding)

This example shows how to enable RPF encoding using IETF standard:

```
(config)# router pim
(config-pim-default-ipv4)# address-family ipv4
(config-pim-default-ipv4)# rpf-vector use-standard-encoding
!
(config)# multicast-routing
(config-mcast)# interface TenGigE0/0/0/0
(config-mcast)# interface TenGigE0/0/0/2
```

Verification

```
Router#show pim neighbor
Tue Apr 17 10:15:40.961 PDT
```

```
PIM neighbors in VRF default
Flag: B - Bidir capable, P - Proxy capable, DR - Designated Router,
      E - ECMP Redirect capable
      * indicates the neighbor created for this router
```

Neighbor Address	Interface	Uptime	Expires	DR pri	Flags
25.25.25.1	TenGigE0/0/0/0	1w3d	00:01:36	1	B P
25.25.25.2*	TenGigE0/0/0/0	1w3d	00:01:41	1 (DR)	B P E
32.32.32.2*	TenGigE0/0/0/2	1w4d	00:01:40	1	B P E
32.32.32.3	TenGigE0/0/0/2	1w4d	00:01:42	1 (DR)	B P

In the above output, you can see "P" tag on the multicast enabled interfaces.

PIM Bootstrap Router

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

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

To avoid a single point of failure, you can configure several candidate BSRs in a PIM domain. A BSR is elected among the candidate BSRs automatically.

Candidates use bootstrap messages to discover which BSR has the highest priority. The candidate with the highest priority sends an announcement to all PIM routers in the PIM domain that it is the BSR.

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

Configuring PIM Bootstrap Router

Configuration Example

Configures the router as a candidate BSR with a hash mask length of 30:

```
Router#config
Router(config)#router pim
Router(config-pim-default-ipv4)#bsr candidate-bsr 1.1.1.1 hash-mask-len 30 priority 1
Router(config-pim-default-ipv4-if)#commit
```

Configures the router to advertise itself as a candidate rendezvous point to the BSR in its PIM domain. Access list number 4 specifies the prefix associated with the candidate rendezvous point address 1.1.1.1. This rendezvous point is responsible for the groups with the prefix 239.

```
Router#config
Router(config)#router pim
Router(config-pim-default-ipv4)#bsr candidate-rp 1.1.1.1 group-list 4 priority 192 interval 60

Router(config-pim-default-ipv4)#exit
Router(config)#ipv4 access-list 4
Router(config-ipv4-acl)#permit ipv4 any 239.0.0.0 0.255.255.255
Router(config-ipv4-acl)#commit
```

Running Configuration

```
Router#show run router pim
router pim
 address-family ipv4
   bsr candidate-bsr 1.1.1.1 hash-mask-len 30 priority 1
   bsr candidate-rp 1.1.1.1 group-list 4 priority 192 interval 60
```

Verification

```
Router#show pim rp mapping
PIM Group-to-RP Mappings
Group(s) 239.0.0.0/8
  RP 1.1.1.1 (?), v2
    Info source: 1.1.1.1 (?), elected via bsr, priority 192, holdtime 150
    Uptime: 00:02:50, expires: 00:01:54

Router#show pim bsr candidate-rp
PIM BSR Candidate RP Info
Cand-RP      mode  scope priority uptime    group-list
1.1.1.1      BD    16     192     00:04:06  4

Router#show pim bsr election
PIM BSR Election State
Cand/Elect-State      Uptime    BS-Timer    BSR                               C-BSR
Elected/Accept-Pref  00:03:49  00:00:25  1.1.1.1 [1, 30]                  1.1.1.1 [1, 30]
```

PIM-Source Specific Multicast

When PIM is used in SSM mode, multicast routing is easier to manage. This is because RPs (rendezvous points) are not required and therefore, no shared trees (*,G) are built.

There is no specific IETF document defining PIM-SSM. However, RFC4607 defines the overall SSM behavior.

In the rest of this document, we use the term PIM-SSM to describe PIM behavior and configuration when SSM is used.

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

- By default, PIM-SSM operates in the 232.0.0.0/8 multicast group range for IPv4 and FF3x::/32 for IPv6. To configure these values, use the **ssm range** command.
- If SSM is deployed in a network already configured for PIM-SM, only the last-hop routers must be upgraded with Cisco IOS XR Software that supports the SSM feature.
- No MSDP SA messages within the SSM range are accepted, generated, or forwarded.
- SSM can be disabled using the **ssm disable** command.
- The **ssm allow-override** command allows SSM ranges to be overridden by more specific ranges.

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

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

To run SSM with IGMPv3, SSM must be supported on the multicast router, the host where the application is running, and the application itself. Cisco IOS XR Software allows SSM configuration for an arbitrary subset of the IP multicast address range 224.0.0.0 through 239.255.255.255.

When an SSM range is defined, existing IP multicast receiver applications do not receive any traffic when they try to use addresses in the SSM range, unless the application is modified to use explicit (S,G) channel subscription.

Benefits of PIM-SSM over PIM-SM

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

IGMPv2

To support IGMPv2, SSM mapping configuration must be added while configuring IGMP to match certain sources to group range.

Configuring Example

Configures the access-list (mc1):

```
Router#configure
Router(config)#ipv4 access-list mc1
Router(config-ipv4-acl)#permit ipv4 any 232.1.1.0 0.0.0.255
Router(config-ipv4-acl)#commit
```

Configures the multicast source (1.1.1.1) as part of a set of sources that map SSM groups described by the specified access-list (mc1):

```
Router#configure
Router(config)#router igmp
Router(config-igmp)#ssm map static 1.1.1.1 mc1
Router(config-igmp)#commit
```

Running Configuration

```
Router#show run router igmp
router igmp
ssm map static 1.1.1.1 mc1
```

Multipath Option

The multipath option is available under `router pim` configuration mode. After multipath option is enabled, SSM selects different path to reach same destination instead of choosing common path. The multipath option helps load balance the SSM traffic.

Configuring Multipath Option

```
Router#configure
Router(config)#router pim address-family ipv4
Router(config-pim-default-ipv4)#multipath hash source
Router(config-pim-default-ipv4)#commit
```

Running Configuration

```
Router#show running router pim
router pim
address-family ipv4
dr-priority 100
multipath hash source /*SSM traffic takes different path to reach same destination
based on source hash value.*/
```

Verification

The Bundle-Ether132 and TenGigE0/4/0/18/0.132 are two paths to reach the destination router Turnin-56. Since we have enabled multipath option, the source has two IP addresses 50.11.30.12 and 50.11.30.11. The Multicast traffic from two sources take two different paths Bundle-Ether132 and TenGigE0/4/0/18/0.132 to reach same destination.

This show run output shows that Bundle-Ether132 and TenGigE0/4/0/18/0.132 are connected to same destination router Turin-56:

```

Router#show run int TenGigE0/1/0/6/3.132
interface TenGigE0/1/0/6/3.132
  description Connected to Turin-56 ten0/0/0/19.132
  ipv4 address 13.0.2.1 255.255.255.240
  ipv6 address 2606::13:0:2:1/120
  encapsulation dot1q 132
!

Router#show run int be132
interface Bundle-Ether132
  description Bundle between Fretta-56 and Turin-56
  ipv4 address 28.0.0.1 255.255.255.240
  ipv6 address 2606::28:0:0:1/120
  load-interval 30

Router#show mrib route 50.11.30.11 detail

IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
  C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
  IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
  MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
  CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
  MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
  MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
  NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
  II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
  LD - Local Disinterest, DI - Decapsulation Interface
  EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
  EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
  MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface
  IRMI - IR MDT Interface

(50.11.30.11,225.255.11.1) Ver: 0x523cc294 RPF nbr: 50.11.30.11 Flags: L RPF, FGID: 11453,
-1, -1
  Up: 4d15h
  Incoming Interface List
    HundredGigE0/4/0/10.1130 Flags: A, Up: 4d15h
  Outgoing Interface List
    FortyGigE0/1/0/5 Flags: F NS, Up: 4d15h
    TenGigE0/4/0/6/0 Flags: F NS, Up: 4d15h
    TenGigE0/1/0/6/3.132 Flags: F NS, Up: 4d15h
    TenGigE0/4/0/18/0.122 Flags: F NS, Up: 4d15h

Router#show mrib route 50.11.30.12 detail

IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
  C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
  IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
  MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
  CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
  MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
  MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
  NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
  II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
  LD - Local Disinterest, DI - Decapsulation Interface
  EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
  EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
  MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface

```

```

IRMI - IR MDT Interface

(50.11.30.12,226.255.12.1) Ver: 0x5fe02e5b RPF nbr: 50.11.30.12 Flags: L RPF, FGID: 12686,
-1, -1
Up: 4d15h
Incoming Interface List
  HundredGigE0/4/0/10.1130 Flags: A, Up: 4d15h
Outgoing Interface List
  Bundle-Ether121 Flags: F NS, Up: 4d15h
  Bundle-Ether132 Flags: F NS, Up: 4d15h
  FortyGigE0/1/0/5 Flags: F NS, Up: 4d15h
  TenGigE0/4/0/6/0.117 Flags: F NS, Up: 4d15h

```

Configuring PIM-SSM

Configuration Example

Configures SSM service for the IPv4 address range defined by access list 4.

```

Router#config
Router(config)#ipv4 access-list 4
Router(config-ipv4-acl)#permit ipv4 any 224.2.151.0 0.0.0.255
Router(config-ipv4-acl)#exit
Router(config)#multicast-routing
Router(config-mcast)#address-family ipv4
Router(config-mcast-default-ipv4)#ssm range 4
Router(config-mcast-default-ipv4)#commit
Router(config-mcast-default-ipv4)#end

```

Running Configuration

```

Router#show running multicast-routing
multicast-routing
  address-family ipv4
    ssm range 4
  interface all enable
!

```

Verification

Verify if the SSM range is configured according to the set parameters:

```

Router#show access-lists 4
ipv4 access-list 4
  10 permit ipv4 any 224.2.151.0 0.0.0.255

*/Verify if the SSM is configured for 224.2.151.0/24/*:

Router#show pim group-map
IP PIM Group Mapping Table
(* indicates group mappings being used)
Group Range      Proto Client  Groups RP address      Info
224.0.1.39/32*   DM    perm    1    0.0.0.0
224.0.1.40/32*   DM    perm    1    0.0.0.0
224.0.0.0/24*    NO    perm    0    0.0.0.0
224.2.151.0/24* SSM config 0    0.0.0.0

```

Configuring PIM Parameters

To configure PIM-specific parameters, the router pim configuration mode is used. The default configuration prompt is for IPv4 and will be seen as config-pim-default-ipv4. To ensure the election of a router as PIM DR on a LAN segment, use the **dr-priority** command. The router with the highest DR priority will win the election. By default, at a preconfigured threshold, the last hop router can join the shortest path tree to receive multicast traffic. To change this behavior, use the command **spt-threshold infinity** under the router pim configuration mode. This will result in the last hop router permanently joining the shared tree. The frequency at which a router sends PIM hello messages to its neighbors can be configured by the hello-interval command. By default, PIM hello messages are sent once every 30 seconds. If the hello-interval is configured under router pim configuration mode, all the interfaces with PIM enabled will inherit this value. To change the hello interval on the interface, use the **hello-interval** command under interface configuration mode, as follows:

Configuration Example

```
Router#configure
Router (config)#router pim
Router (config-pim-default)#address-family ipv4
Router (config-pim-default-ipv4)#dr-priority 2
Router (config-pim-default-ipv4)#spt-threshold infinity
Router (config-pim-default-ipv4)#interface TenGigE0/11/0/1
Router (config-pim-ipv4-if)#dr-priority 4
Router (config-pim-ipv4-if)#hello-interval 45
Router (config-pim-ipv4-if)#commit
```

Running Configuration

```
Router#show run router pim
router pim
  address-family ipv4
    dr-priority 2
    spt-threshold infinity
  interface TenGigE0/11/0/1
    dr-priority 4
    hello-interval 45
```

Verification

Verify if the parameters are set according to the configured values:

```
Router#show pim interface te0/11/0/1
PIM interfaces in VRF default
Address          Interface      PIM  Nbr  Hello  DR    DR Count Intvl
  Prior
100.1.1.1        TenGigE0/11/0/1  on   1    45    4    this system
```

Multicast Source Discovery Protocol

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

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

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



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

Interconnecting PIM-SM Domains with MSDP

To set up an MSDP peering relationship with MSDP-enabled routers in another domain, you configure an MSDP peer to the local router.

If you do not want to have or cannot have a BGP peer in your domain, you could define a default MSDP peer from which to accept all Source-Active (SA) messages.

Finally, you can change the Originator ID when you configure a logical RP on multiple routers in an MSDP mesh group.

Before you begin

You must configure MSDP default peering, if the addresses of all MSDP peers are not known in BGP or multiprotocol BGP.

Procedure

	Command or Action	Purpose
Step 1	configure	
Step 2	interface <i>type interface-path-id</i> Example: <pre>RP/0/RP0/CPU0:router(config)# interface loopback 0</pre>	(Optional) Enters interface configuration mode to define the IPv4 address for the interface. Note This step is required if you specify an interface type and number whose primary address becomes the source IP address for the TCP connection.
Step 3	ipv4 address <i>address mask</i> Example:	(Optional) Defines the IPv4 address for the interface.

	Command or Action	Purpose
	<pre>RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.0.1.3 255.255.255.0</pre>	<p>Note This step is required only if you specify an interface type and number whose primary address becomes the source IP address for the TCP connection. See optional for information about configuring the connect-source command.</p>
Step 4	<p>exit</p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-if)# end</pre>	Exits interface configuration mode.
Step 5	<p>router msdp</p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config)# router msdp</pre>	Enters MSDP protocol configuration mode.
Step 6	<p>default-peer ip-address [prefix-list list]</p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-msdp)# default-peer 172.23.16.0</pre>	(Optional) Defines a default peer from which to accept all MSDP SA messages.
Step 7	<p>originator-id type interface-path-id</p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-msdp)# originator-id GigabitEthernet0/1/1/0</pre>	(Optional) Allows an MSDP speaker that originates a (Source-Active) SA message to use the IP address of the interface as the RP address in the SA message.
Step 8	<p>peer peer-address</p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-msdp)# peer 172.31.1.2</pre>	<p>Enters MSDP peer configuration mode and configures an MSDP peer.</p> <ul style="list-style-type: none"> • Configure the router as a BGP neighbor. • If you are also BGP peering with this MSDP peer, use the same IP address for MSDP and BGP. You are not required to run BGP or multiprotocol BGP with the MSDP peer, as long as there is a BGP or multiprotocol BGP path between the MSDP peers.

	Command or Action	Purpose
Step 9	connect-source <i>type interface-path-id</i> Example: <pre>RP/0/RP0/CPU0:router(config-msdp-peer)# connect-source loopback 0</pre>	(Optional) Configures a source address used for an MSDP connection.
Step 10	mesh-group <i>name</i> Example: <pre>RP/0/RP0/CPU0:router(config-msdp-peer)# mesh-group internal</pre>	(Optional) Configures an MSDP peer to be a member of a mesh group.
Step 11	remote-as <i>as-number</i> Example: <pre>RP/0/RP0/CPU0:router(config-msdp-peer)# remote-as 250</pre>	(Optional) Configures the remote autonomous system number of this peer.
Step 12	commit	
Step 13	show msdp [ipv4] globals Example: <pre>RP/0/RP0/CPU0:router# show msdp globals</pre>	Displays the MSDP global variables.
Step 14	show msdp [ipv4] peer [peer-address] Example: <pre>RP/0/RP0/CPU0:router# show msdp peer 172.31.1.2</pre>	Displays information about the MSDP peer.
Step 15	show msdp [ipv4] rpf rpf-address Example: <pre>RP/0/RP0/CPU0:router# show msdp rpf 172.16.10.13</pre>	Displays the RPF lookup.

Controlling Source Information on MSDP Peer Routers

Your MSDP peer router can be customized to control source information that is originated, forwarded, received, cached, and encapsulated.

When originating Source-Active (SA) messages, you can control to whom you will originate source information, based on the source that is requesting information.

When forwarding SA messages you can do the following:

- Filter all source/group pairs
- Specify an extended access list to pass only certain source/group pairs
- Filter based on match criteria in a route map

When receiving SA messages you can do the following:

- Filter all incoming SA messages from an MSDP peer
- Specify an extended access list to pass certain source/group pairs
- Filter based on match criteria in a route map

In addition, you can use time to live (TTL) to control what data is encapsulated in the first SA message for every source. For example, you could limit internal traffic to a TTL of eight hops. If you want other groups to go to external locations, you send those packets with a TTL greater than eight hops.

By default, MSDP automatically sends SA messages to peers when a new member joins a group and wants to receive multicast traffic. You are no longer required to configure an SA request to a specified MSDP peer.

Procedure

	Command or Action	Purpose
Step 1	configure	
Step 2	router msdp Example: RP/0/RP0/CPU0:router(config)# router msdp	Enters MSDP protocol configuration mode.
Step 3	sa-filter {in out} [list access-list-name] [rp-list access-list-name] Example: RP/0/RP0/CPU0:router(config-msdp)# sa-filter out list 100	Configures an incoming or outgoing filter list for messages received from the specified MSDP peer. <ul style="list-style-type: none"> • If you specify both the list and rp-list keywords, all conditions must be true to pass any source, group (S, G) pairs in outgoing Source-Active (SA) messages. • You must configure the ipv4 access-list command in Step 7, on page 19. • If all match criteria are true, a permit from the route map passes routes through the filter. A deny filters routes.

	Command or Action	Purpose
Step 4	cache-sa-state [<i>list access-list-name</i>] [<i>rp-list access-list-name</i>] Example: <pre>RP/0/RP0/CPU0:router(config-msdp)# cache-sa-state list 100</pre>	Creates and caches source/group pairs from received Source-Active (SA) messages and controls pairs through access lists.
Step 5	ttl-threshold <i>ttl-value</i> Example: <pre>RP/0/RP0/CPU0:router(config-msdp)# ttl-threshold 8</pre>	(Optional) Limits which multicast data is sent in SA messages to an MSDP peer. <ul style="list-style-type: none"> • Only multicast packets with an IP header TTL greater than or equal to the <i>ttl-value</i> argument are sent to the MSDP peer specified by the IP address or name. • Use this command if you want to use TTL to examine your multicast data traffic. For example, you could limit internal traffic to a TTL of 8. If you want other groups to go to external locations, send those packets with a TTL greater than 8. • This example configures a TTL threshold of eight hops.
Step 6	exit Example: <pre>RP/0/RP0/CPU0:router(config-msdp)# exit</pre>	Exits the current configuration mode.
Step 7	ipv4 access-list <i>name</i> [<i>sequence-number</i>] permit <i>source</i> [<i>source-wildcard</i>] Example: <pre>RP/0/RP0/CPU0:router(config)# ipv4 access-list 100 20 permit 239.1.1.1 0.0.0.0</pre>	Defines an IPv4 access list to be used by SA filtering. <ul style="list-style-type: none"> • In this example, the access list 100 permits multicast group 239.1.1.1. • The ipv4 access-list command is required if the keyword list is configured for SA filtering in Step 3, on page 18.
Step 8	commit	

PIM-Sparse Mode

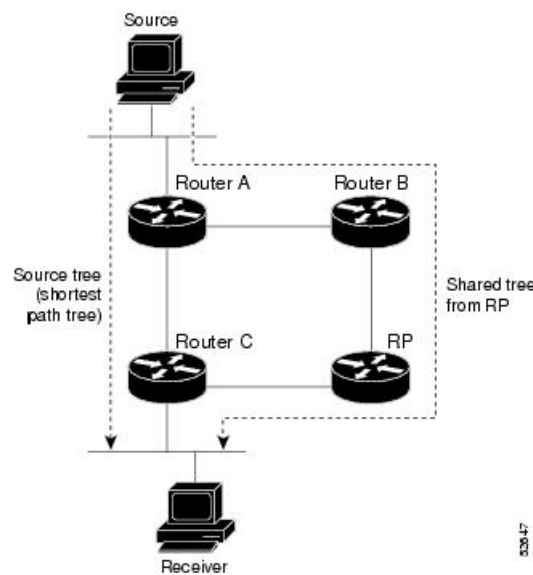
Typically, PIM in sparse mode (PIM-SM) operation is used in a multicast network when relatively few routers are involved in each multicast. Routers do not forward multicast packets for a group, unless there is an explicit request for traffic. Requests are accomplished using PIM join messages, which are sent hop by hop toward

the root node of the tree. The root node of a tree in PIM-SM is the rendezvous point (RP) in the case of a shared tree or the first-hop router that is directly connected to the multicast source in the case of a shortest path tree (SPT). The RP keeps track of multicast groups, and the sources that send multicast packets are registered with the RP by the first-hop router of the source.

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

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

Figure 1: Shared Tree and Source Tree (Shortest Path Tree)



In PIM-SM, the rendezvous point (RP) is used to bridge sources sending data to a particular group with receivers sending joins for that group. In the initial set up of state, interested receivers receive data from senders to the group across a single data distribution tree rooted at the RP. This type of distribution tree is called a shared tree or rendezvous point tree (RPT) as illustrated in Figure 4: Shared Tree and Source Tree (Shortest Path Tree), above. Data from senders is delivered to the RP for distribution to group members joined to the shared tree.

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

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

1. Receiver joins a group; leaf Router C sends a join message toward RP.
2. RP puts link to Router C in its outgoing interface list.
3. Source sends data; Router A encapsulates data in Register and sends it to RP.

4. RP forwards data down the shared tree to Router C and sends a join message toward Source. At this point, data may arrive twice at the RP, once encapsulated and once natively.
5. When data arrives natively (unencapsulated) at RP, RP sends a register-stop message to Router A.
6. By default, receipt of the first data packet prompts Router C to send a join message toward Source.
7. When Router C receives data on (S,G), it sends a prune message for Source up the shared tree.
8. RP deletes the link to Router C from outgoing interface of (S,G). RP triggers a prune message toward Source.
9. Join and prune messages are sent for sources and RPs. They are sent hop by hop and are processed by each PIM router along the path to the source or RP. Register and register-stop messages are not sent hop by hop. They are exchanged using direct unicast communication between the designated router that is directly connected to a source and the RP for the group.



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

Designated Routers

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

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

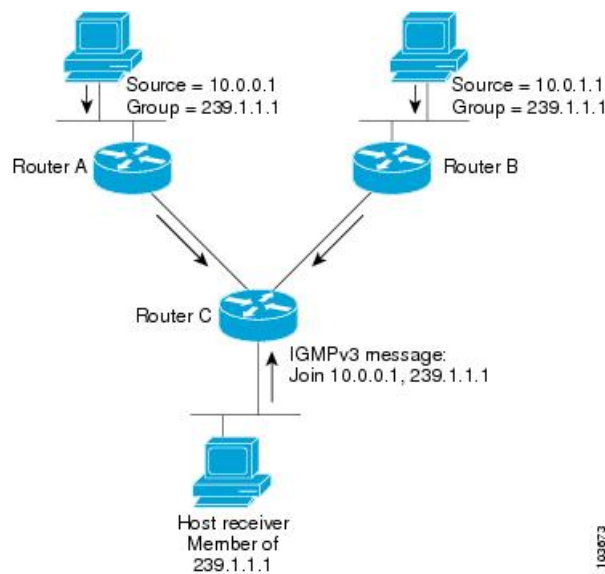
If there are multiple PIM routers on a LAN, a designated router must be elected to avoid duplicating multicast traffic for connected hosts. The PIM router with the highest IP address becomes the DR for the LAN unless you choose to force the DR election by use of the **dr-priority** command. The DR priority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



Note DR election process is required only on multi access LANs. The last-hop router directly connected to the host is the DR.

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

Figure 2: Designated Router Election on a Multiaccess Segment



If the DR fails, the PIM provides a way to detect the failure of Router A and to elect a failover DR. If the DR (Router A) were to become inoperable, Router B would detect this situation when its neighbor adjacency with Router A timed out. Because Router B has been hearing IGMP membership reports from Host A, it already has IGMP state for Group A on this interface and immediately sends a join to the RP when it becomes the new DR. This step reestablishes traffic flow down a new branch of the shared tree using Router B. Additionally, if Host A were sourcing traffic, Router B would initiate a new register process immediately after receiving the next multicast packet from Host A. This action would trigger the RP to join the SPT to Host A, using a new branch through Router B.



Note Two PIM routers are neighbors if there is a direct connection between them. To display your PIM neighbors, use the `show pim neighbor` command in EXEC mode.

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

Configuration Example

Configures the router to use DR priority 4 for TenGigE interface 0/11/0/1, but other interfaces will inherit DR priority 2:

```
Router#configure
Router(config)#router pim
```

```

Router(config-pim-default) #address-family ipv4
Router(config-pim-default-ipv4) #dr-priority 2
Router(config-pim-default-ipv4) #interface TenGigE0/11/0/1
Router(config-pim-ipv4-if) #dr-priority 4
Router(config-ipv4-acl) #commit

```

Running Configuration

```

Router#show run router pim
router pim
address-family ipv4
dr-priority 2
spt-threshold infinity
interface TenGigE0/11/0/1
dr-priority 4
hello-interval 45

```

Verification

Verify if the parameters are set according to the configured values:

```

Router#show pim interface
PIM interfaces in VRF default
Address          Interface          PIM Nbr  Hello  DR   DR Count Intvl  Prior
100.1.1.1        TenGigE0/11/0/1   on   1     45    4   this system

```

Internet Group Management Protocol

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

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

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



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

Restrictions

IGMP snooping under VPLS bridge domain is not supported.

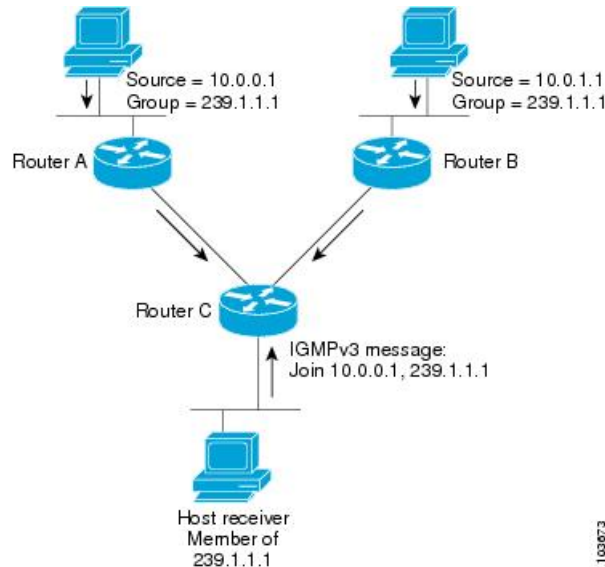
Functioning of IGMP Routing

The following image "IGMP Singaling" , illustrates two sources, 10.0.0.1 and 10.0.1.1, that are multicasting to group 239.1.1.1.

The receiver wants to receive traffic addressed to group 239.1.1.1 from source 10.0.0.1 but not from source 10.0.1.1.

The host must send an IGMPv3 message containing a list of sources and groups (S, G) that it wants to join and a list of sources and groups (S, G) that it wants to leave. Router C can now use this information to prune traffic from Source 10.0.1.1 so that only Source 10.0.0.1 traffic is being delivered to Router C.

Figure 3: IGMP Signaling



Configuring Maximum IGMP Per Interface Group Limit

The IGMP Per Interface States Limit sets a limit on creating OIF for the IGMP interface. When the set limit is reached, the group is not accounted against this interface but the group can exist in IGMP context for some other interface.

- If a user has configured a maximum of 20 groups and has reached the maximum number of groups, then no more groups can be created. If the user reduces the maximum number of groups to 10, the 20 joins will remain and a message of reaching the maximum is displayed. No more joins can be added until the number of groups has reached less than 10.
- If a user already has configured a maximum of 30 joins and add a max of 20, the configuration occurs displaying a message that the maximum has been reached. No state change occurs and also no more joins can occur until the threshold number of groups is brought down below the maximum number of groups.

Configuration Example

Configures all interfaces with 4000 maximum groups per interface except TenGigE interface 0/11/0/0, which is set to 3000:

```
Router#config
Router(config)#router igmp
Router(config-igmp)#maximum groups-per-interface 4000
Router(config-igmp)#interface TenGigE0/11/0/0
Router(config-igmp-default-if)#maximum groups-per-interface 3000
Router(config-igmp-default-if)#commit
```


Running Configuration

```
router igmp
 interface TenGigE0/11/0/0
   maximum groups-per-interface 3000
 !
 maximum groups-per-interface 4000
 !
```

Verification

```
Router#show igmp summary
Robustness Value 2
No. of Group x Interfaces 37
Maximum number of Group x Interfaces 50000
Supported Interfaces : 9
Unsupported Interfaces: 0
Enabled Interfaces : 8
Disabled Interfaces : 1
MTE tuple count : 0
Interface          Number  Max #
                   Groups  Groups
Loopback0          4       4000
TenGigE0/11/0/0    5       4000
TenGigE0/11/0/1    5       4000
TenGigE0/11/0/2    0       4000
TenGigE0/11/0/3    5       4000
TenGigE0/11/0/4    5       3000
TenGigE0/11/0/5    5       4000
TenGigE0/11/0/6    5       4000
TenGigE0/11/0/6.1  3       4000
```

SSM Static Source Mapping

Configure a source (1.1.1.1) as part of a set of sources that map SSM groups described by the specified access-list (4).

Configuration Example

```
Router#configure
Router(config)#ipv4 access-list 4
Router(config-ipv4-acl)#permit ipv4 any 229.1.1.0 0.0.0.255
Router(config-ipv4-acl)#exit
Router(config)# multicast-routing
Router(config-mcast)#address-family ipv4
Router(config-mcast-default-ipv4)#ssm range 4
Router(config-mcast-default-ipv4)#exit
Router(config-mcast)#exit
Router(config)#router igmp
Router(config-igmp)#ssm map static 1.1.1.1 4
*/Repeat the above step as many times as you have source addresses to include in the set
for SSM mapping/*
Router(config-igmp)#interface TenGigE0/11/0/3
Router(config-igmp-default-if)#static-group 229.1.1.1
Router(config-igmp-default-if)#commit
```

Running Configuration

```
Router#show run multicast-routing
multicast-routing
 address-family ipv4
```

```

    ssm range 4
    interface all enable
    !
    !
Router#show access-lists 4
ipv4 access-list 4
 10 permit ipv4 any 229.1.1.0 0.0.0.255

Router#show run router igmp
router igmp
 interface TenGigE0/11/0/3
 static-group 229.1.1.1
 !
 ssm map static 1.1.1.1 4

```

Verification

Verify if the parameters are set according to the configured values:

```

Router#show mrib route 229.1.1.1 detail
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
  C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
  IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
  MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
  CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
  MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
  MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
  NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
  II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
  LD - Local Disinterest, DI - Decapsulation Interface
  EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
  EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
  MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface
  IRMI - IR MDT Interface
(1.1.1.1,229.1.1.1) RPF nbr: 1.1.1.1 Flags: RPF
Up: 00:01:11
Incoming Interface List
  Loopback0 Flags: A, Up: 00:01:11
Outgoing Interface List
  TenGigE0/11/0/3 Flags: F NS LI, Up: 00:01:11

```

Information About IGMP Snooping Configuration Profiles

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

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

- Any IGMP profile attached to a bridge domain, even an empty profile, enables IGMP snooping. To disable IGMP snooping, detach the profile from the bridge domain.
- An empty profile configures IGMP snooping on the bridge domain and all ports under the bridge using default configuration settings.
- A bridge domain can have only one IGMP snooping profile attached to it (at the bridge domain level) at any time. Profiles can be attached to ports under the bridge, one profile per port.

- Port profiles are not in effect if the bridge domain does not have a profile attached to it.
- IGMP snooping must be enabled on the bridge domain for any port-specific configurations to be in effect.
- If a profile attached to a bridge domain contains port-specific configuration options, the values apply to all of the ports under the bridge, including all mrouter and host ports, unless another port-specific profile is attached to a port.
- When a profile is attached to a port, IGMP snooping reconfigures that port, disregarding any port configurations that may exist in the bridge-level profile.

**Note**

- IEEE 802.1Q, Q-in-Q, default and untagged encapsulations are supported.
- IEEE 802.1ad and other encapsulations are not supported.
- IEEE 802.1ad is not supported with BVI.

Creating Profiles

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

Attaching and Detaching Profiles

To attach a profile to a bridge domain, use the **mldp snooping profile** command in l2vpn bridge group bridge domain configuration mode. To attach a profile to a port, use the **mldp snooping profile** command in the interface configuration mode under the bridge domain. To detach a profile, use the **no** form of the command in the appropriate configuration mode.

When you detach a profile from a bridge domain or a port, the profile still exists and is available for use at a later time. Detaching a profile has the following results:

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

Changing Profiles

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

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

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

Configuring Access Control

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

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

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

IGMP Snooping Access Groups

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

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



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

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

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

IGMP Snooping Group Weighting

To limit the number of IGMP v2/v3 groups, in which the maximum number of concurrently allowed multicast channels must be configurable on a per EFP-basis and per PW-basis, configure group weighting.

IGMP snooping limits the membership on a bridge port to a configured maximum, but extends the feature to support IGMPv3 source groups and to allow different weights to be assigned to individual groups or source groups. This enables the IPTV provider, for example, to associate standard and high-definition IPTV streams, as appropriate, to specific subscribers.

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

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

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



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

The group limit policy configuration is based on these conditions:

- Group weight values for <*,G> and <S,G> membership are configured in a Route Policy, that is included in an igmp snooping profile attached to a BD or port.
- Port level weight policy overrides any bridge domain level policy, if group-limit is set and route-policy is configured.
- If there is no policy configured, each group weight is counted equally and is equal to 1.
- If policy has been configured, all matching groups get weight of 1 and un-matched groups have 0 weight.

IPv6 Multicast for Multiple Sources

Statistics for Ingress Multicast Routes

Multicast and interface statistics are often used for accounting purpose. By default Multicast Forwarding Information Base (MFIB) does not store multicast route statistics. In order to enable MFIB to create and store multicast route statistics for ingress flows use the **hw-module profile mfib statistics** command in the configuration mode. Use No form of the latter command to disable logging of multicast route statistics. For the configuration to take effect, you must reload affected line cards after executing the command .



Note The MFIB counter can store a maximum of 2000 multicast routes, if the count exceeds beyond 2000 routes, then statistics are overwritten.

This table lists commands used to display or reset multicast route statistics stored in MFIB.

Table 1: show and clear commands for Multicast Statistics

Command	Description
show mfib hardware route statistics location <node-id>	Displays platform-specific MFIB information for the packet and byte counters for all multicast route.
show mfib hardware route <source-address> location <node-id>	Displays platform-specific MFIB information for the packet and byte counters for multicast routes originating from the specified source.
Show mfib hardware route <source-address><group-address> location <node-id>	Displays platform-specific MFIB information for the packet and byte counters for multicast routes originating from the specified source and belonging to specified multicast group.
clear mfib hardware ingress route statistics location <node-id>	Resets allocated counter values regardless of the MFIB hardware statistics mode from the designated node.
clear mfib hardware route <source-address> location <node-id>	Resets allocated counter values regardless of the MFIB hardware statistics mode from the designated node for specified multicast route source.

Command	Description
clear mfib hardware route <source-address><group-address> location <node-id>	Resets allocated counter values regardless of the MFIB hardware statistics mode from the designated node for specified multicast route source and multicast group.



Note To program IPv6 multicast routes in external TCAM, use the following commands:

- **hw-module profile tcam fib v6mcast percent** *value*
- **hw-module profile tcam fib ipv6 unicast percent** *value*
- **hw-module profile tcam fib ipv6 unicast prefix** *value*

Configuring only **hw-module profile tcam fib v6mcast percent** *value* causes an unexpected behaviour for 5501-SE.

Configuring Statistics for Ingress Multicast Routes

Configuration Example

In this example you will enable MRIB route statistics logging for ingress multicast routes for all locations:

```
Router#config
Router(config)#hw-module profile mfib statistics
Router(config)#commit
Router(config)#exit
Router#admin
Router(admin)#reload location all /*Reloads all line cards. This is required step,
else the multicast route statistics will not be created.*/
```

Running Configuration

```
Router#show running config
hw-module profile mfib statistics
!
```

Verification

The below show commands display the multicast statistics for source (192.0.2.2), group (226.1.2.1) and node location 0/RP0/cpu0 for ingress route:



Note The multicast egress statistics per flow (per SG) is not supported. But egress interface level multicast statistics is supported. Also the drop statistics is not supported.

```
Router#show mfib hardware route statistics location 0/RP0/cpu0
(192.0.2.2, 226.1.2.1) :: Packet Stats 109125794 Byte Stats 23680297298
(192.0.2.2, 226.1.2.2) :: Packet Stats 109125760 Byte Stats 23680289920
(192.0.2.2, 226.1.2.3) :: Packet Stats 109125722 Byte Stats 23680281674
(192.0.2.2, 226.1.2.4) :: Packet Stats 109125683 Byte Stats 23680273211
```

```
(192.0.2.2, 226.1.2.5) :: Packet Stats 109125644 Byte Stats 23680264748
(192.0.2.2, 226.1.2.6) :: Packet Stats 109129505 Byte Stats 23681102585
(192.0.2.2, 226.1.2.7) :: Packet Stats 109129470 Byte Stats 23681094990
(192.0.2.2, 226.1.2.8) :: Packet Stats 109129428 Byte Stats 23681085876
(192.0.2.2, 226.1.2.9) :: Packet Stats 109129385 Byte Stats 23681076545
(192.0.2.2, 226.1.2.10) :: Packet Stats 109129336 Byte Stats 23681065912
```

```
Router#show mfib hardware route statistics 192.0.2.2 location 0/RP0/cpu0
(192.0.2.2, 226.1.2.1) :: Packet Stats 109184295 Byte Stats 23692992015
(192.0.2.2, 226.1.2.2) :: Packet Stats 109184261 Byte Stats 23692984637
(192.0.2.2, 226.1.2.3) :: Packet Stats 109184223 Byte Stats 23692976391
(192.0.2.2, 226.1.2.4) :: Packet Stats 109184184 Byte Stats 23692967928
(192.0.2.2, 226.1.2.5) :: Packet Stats 109184145 Byte Stats 23692959465
(192.0.2.2, 226.1.2.6) :: Packet Stats 109184106 Byte Stats 23692951002
(192.0.2.2, 226.1.2.7) :: Packet Stats 109184071 Byte Stats 23692943407
(192.0.2.2, 226.1.2.8) :: Packet Stats 109184029 Byte Stats 23692934293
(192.0.2.2, 226.1.2.9) :: Packet Stats 109183986 Byte Stats 23692924962
```

```
Router#show mfib hardware route statistics 192.0.2.2 226.1.2.1 location 0/RP0/cpu0
(192.0.2.2, 226.1.2.1) :: Packet Stats 109207695 Byte Stats 23698069815
```

Multicast Route Statistics

Multicast route statistic feature provides information about the multicast routes. The multicast statistics information includes the rate at which packets are received.

Before enabling multicast route statistics, you must configure an ACL to specify which of the IP route statistics to be captured.

Restrictions for Implementing Multicast Route Statistics Feature

These are the points that you should consider before implementing multicast route statistics feature:

- Multicast route statistics are available for <S,G> routes only. The statistics for <*,G> routes are not available.
- IPv6 multicast route statistics are not supported.
- Multicast route statistics for egress direction is not supported.
- When ACL is mapped with **hw-module router-stats** configuration, you can't modify the ACL. To modify ACLs that are mapped with router-stats, remove the existing **hw-module router-stats** configuration and update the ACL entries. Then, configure the **hw-module router-stats** again.

This feature supports only:

- L3 Multicast traffic.
- Default VRFs.

Configure Multicast Route Statistics

Configuring multicast route statistics includes these main tasks:

- Configuring an ACL

- Enabling multicast route statistics for the configured ACLs

```
RP0/0/RP0/CPU0:router# configure

/* Configure an ACL matching the (S,G) routes for which statistics have to be captured:*/
RP0/0/RP0/CPU0:router(config)# ipv4 access-list mcast-counter
RP0/0/RP0/CPU0:router(config-acl)# 10 permit ipv4 host 10.1.1.2 host 224.2.151.1
RP0/0/RP0/CPU0:router(config-acl)# 30 permit ipv4 10.1.1.0/24 232.0.4.0/22
RP0/0/RP0/CPU0:router(config-acl)# 50 permit ipv4 192.168.0.0/24 232.0.4.0/22
RP0/0/RP0/CPU0:router(config-acl)#commit
RP0/0/RP0/CPU0:router(config-acl)#exit

/* Enable multicast route statistics for the configured ACL on the default VRF. */
RP0/0/RP0/CPU0:router(config)# hw-module route-stats l3mcast vrf default ipv4 egress
mcast-router
RP0/0/RP0/CPU0:router(config)# hw-module route-stats l3mcast vrf default ipv4 ingress
mcast-router
```



Note

- If you are enabling the route stats for a router on the global table, use **vrf default**. If you are enabling the route stats for specific vrf, use the **vrf vrfname** option.
- In case, you want to enable route stats for all tables, do not use the **vrf**.

For example:

```
RP0/0/RP0/CPU0:router(config)#hw-module route-stats l3mcast ipv4 mcast-counter
```

Verification

Use the **show mfib route rate** command to verify if the multicast route information is captured for the traffic that matches the ACL:



Note The ingress stats are always per S, G.

```
RP0/0/RP0/CPU0:router# show mfib route rate
Thu Aug 16 18:04:47.312 PDT

IP Multicast Forwarding Rates
(Source Address, Group Address)
  Incoming rate:
    Node: (Incoming node) : pps/bps
  Outgoing rate:
    Node: (Outgoing node) : pps/bps

(10.1.1.2,232.0.0.1)
  Incoming rate :
    Node : 0/0/CPU0 : 4593 / 18153671
  Outgoing rate :
    Node : 0/0/CPU0 : 0 / 0
```

The above output shows that the multicast source **10.1.1.2** is sending packets to multicast group **232.0.0.1** and is received at **4593** pps.

For the information on the interface accounting stats, use the show interface accounting command. The following show command displays interface accounting stats for ingress:

```
Router# show int tenGigE 0/0/0/15 accounting
Mon Nov 12 10:26:20.592 UTC
TenGigE0/0/0/15
  Protocol          Pkts In          Chars In          Pkts Out          Chars Out
  IPV6_MULTICAST    22125711958      1814308380556     0                  0
  IPV6_ND            0                 0                  1243               128960
```

Cisco IOS XR Release 7.4.1 and later support YANG data model for multicast interface counters.

- Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/protocols/protocol
- Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface[interface-name=TenGigE0/0/18]/protocols/protocol



Note The YANG model does not support ingress and egress multicast route stats.

The following show command displays interface accounting stats for egress:

```
Router# show interfaces bundle-ether 100.1001 accounting rates
Mon Aug 26 15:56:41.738 IST
Bundle-Ether100.1001
          Ingress
Protocol          Bits/sec          Pkts/sec          Bits/sec          Pkts/sec
  IPV4_MULTICAST    0                  0                 11455000           990
  IPV6_MULTICAST    0                  0                 11455000           990
  ARP                0                  0                  0                  0
  IPV6_ND            0                  0                  0                  0
          Egress
```

Use Case: Video Streaming

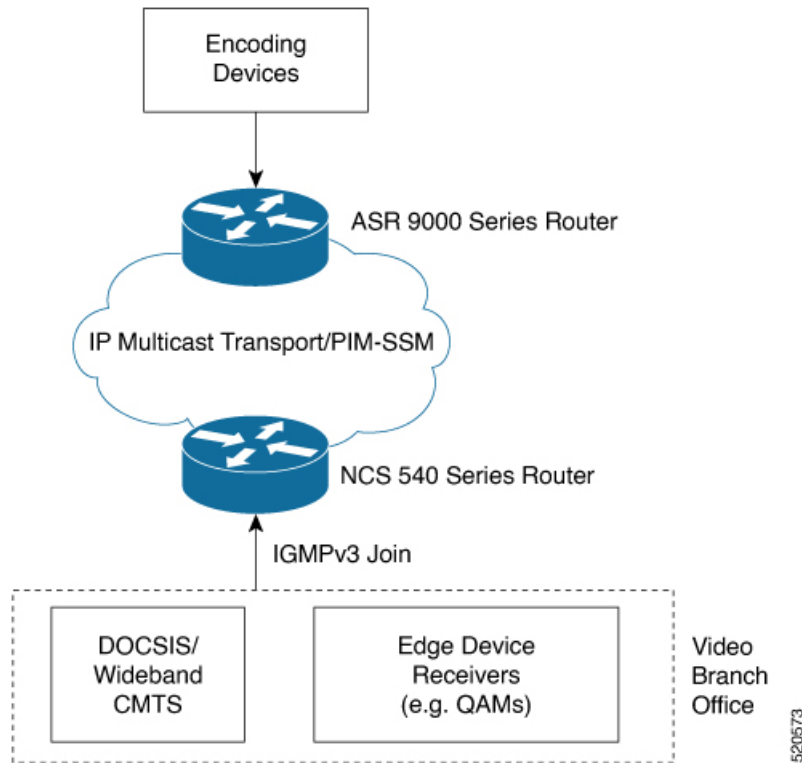
In today's broadcast video networks, proprietary transport systems are used to deliver entire channel line-ups to each video branch office. IP based transport network would be a cost efficient/convenient alternative to deliver video services combined with the delivery of other IP based services. (Internet delivery or business services)

By its very nature, broadcast video is a service well-suited to using IP multicast as a more efficient delivery mechanism to reach end customers.

The IP multicast delivery of broadcast video is explained as follows:

1. Encoding devices in digital primary headends, encode one or more video channels into a Moving Pictures Expert Group (MPEG) stream which is carried in the network via IP multicast.
2. Devices at video branch office are configured by the operator to request the desired multicast content via IGMP joins.
3. The network, using PIM-SSM as its multicast routing protocol, routes the multicast stream from the digital primary headend to edge device receivers located in the video branch office. These edge devices could be edge QAM devices which modulate the MPEG stream for an RF frequency, or CMTS for DOCSIS.

Figure 4: Video Streaming



Multicast over Access Pseudo-Wire

Multicast over access pseudo-wire (PW) allow multicast traffic flooding with MLDP core and PWs that are terminating at CEs. Therefore, connecting two IGMP domains and extending the MVPN traffic via MPLS network terminating at a Layer 3 (VRF or global) domain or a Layer 2 domain using PW.

Multicast over access PWs help service providers to scale and reduce the hardware cost.



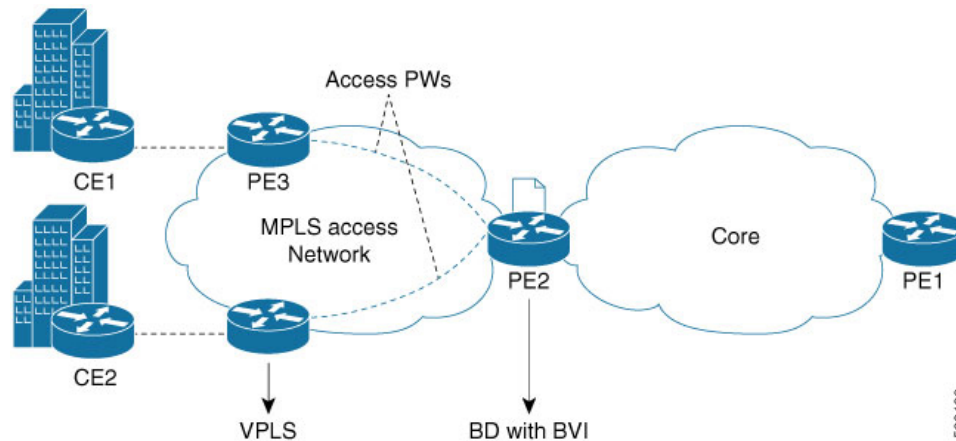
Note This feature isn't supported on the NCS 560 router.

Implementation Consideration

- Doesn't support IGMP and MLD snooping over access PW
- Supports only flood mode
- Supports only SSM routes
- Doesn't support QoS over access PW (ingress/egress)
- Configure maximum MTU on the device acting as access PW endpoint. This allows easy movement of protocol packets.

Configuring Multicast Over Access Pseudo-Wire

Consider the sample topology as shown in the below figure.



In the above topology:

- CEs are connected to PE3 (access device). PE3 has access PW configured. PE3 is reachable at 192.127.0.1
- PE2 (NCS 5500 or NCS 540) has VPLS configured with BVI and access PW.
- A point-to-multi point connectivity is established between PE2 and PE3s via pseudo-wire with BD and BVI interface.
- Multicast packets received from CEs over access PW are sent to PE2 with BVI as the incoming interface.
- Multicast packets received from the core are replicated over access PW towards PE3, which in turn replicates and forwards to the CEs. Here BVI acts as the forwarding interface.

The sample configuration is shown below:

```

/* Enter global configuration mode */
Router# configure
Router(config)# l2vpn

/* Configure pseudowire class name */
Router(config-l2vpn)# pw-class mpls

/* Configure MPLS encapsulation for the pseudowire */
Router(config-l2vpn-pwc)# encapsulation mpls
Router(config-l2vpn-pwc-mpls)#control-word
Router(config-l2vpn-pwc-mpls)#transport-mode ethernet
Router(config-l2vpn-pwc-mpls)#load-balancing
Router(config-l2vpn-pwc-mpls-load-bal)#flow-label both
Router(config-l2vpn-pwc-mpls-load-bal)#exit
Router(config-l2vpn-pwc-mpls)#exit
Router(config-l2vpn-pwc)#exit

/* Configure bridge group and bridge domain, then assign network interfaces to the bridge domain. */
Router(config-l2vpn)#bridge group bvi-access-pw
Router(config-l2vpn-bg)#bridge-domain 1
Router(config-l2vpn-bg-bd)#interface tengigE 0/0/0/0.1
Router(config-l2vpn-bg-bd-ac)#exit

/* Configure the pseudowire port to the bridge domain and the peer to the bridge domain.

```

```

*/
Router(config-l2vpn-bg-bd)#neighbor 192.127.0.1 pw-id 1
Router(config-l2vpn-bg-bd-pw)#exit
Router(config-l2vpn-bg-bd)#routed interface bvi1
Router(config-l2vpn-bg-bd)# commit

```

Running Config

This section shows the Multicast over Access PW running config:

```

l2vpn
pw-class mpls
  encapsulation mpls
  control-word
  transport-mode ethernet
  load-balancing
  flow-label both
!
!

bridge group BVI-ACCESS-PW
  bridge-domain 1
  interface TenGigE0/0/0/0.1
  !
  vfi 1
  neighbor 192.127.0.1 pw-id 1
  pw-class mpls
  !
  routed interface BVI1
  !

```

Verification

Verify the status of PW using the **show l2vpn bridge-domain** command:

```
RP/0/RP0/CPU0# show l2vpn bridge-domain bd-name 1 detail
```

```

Legend: pp = Partially Programmed.
Bridge group: BVI-ACCESS-PW, bridge-domain: 1, id: 1, state: up, ShgId: 0, MSTi: 0
  Coupled state: disabled
  VINE state: BVI Resolved
  MAC learning: enabled
  MAC withdraw: enabled
    MAC withdraw for Access PW: enabled
    MAC withdraw sent on: bridge port up
    MAC withdraw relaying (access to access): disabled
  Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  MAC limit: 64000, Action: none, Notification: syslog
  MAC limit reached: no, threshold: 75%
  MAC port down flush: enabled
  MAC Secure: disabled, Logging: disabled
  Split Horizon Group: none
  Dynamic ARP Inspection: disabled, Logging: disabled
  IP Source Guard: disabled, Logging: disabled
  DHCPv4 Snooping: disabled
  DHCPv4 Snooping profile: none
  IGMP Snooping: disabled
  IGMP Snooping profile: none
  MLD Snooping profile: none
  Storm Control: disabled
  Bridge MTU: 9086

```

```

MIB cvplsConfigIndex: 2
Filter MAC addresses:
P2MP PW: disabled
Multicast Source: IPv4
Create time: 22/09/2019 15:00:09 (2w5d ago)
No status change since creation
ACs: 2 (2 up), VFIs: 0, PWs: 1 (1 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
List of ACs:
  AC: BV11, state is up
    Type Routed-Interface
    MTU 1514; XC ID 0x800001f7; interworking none
    BVI MAC address:
      0032.1772.20dc
    Split Horizon Group: Access
    PD System Data: AF-LIF-IPv4: 0x00000000 AF-LIF-IPv6: 0x00000000
  AC: TenGigE0/0/0/0.1, state is up
    Type VLAN; Num Ranges: 1
    Rewrite Tags: []
    VLAN ranges: [1, 1]
    MTU 9086; XC ID 0x1; interworking none
    MAC learning: enabled
    Flooding:
      Broadcast & Multicast: enabled
      Unknown unicast: enabled
    MAC aging time: 300 s, Type: inactivity
    MAC limit: 64000, Action: none, Notification: syslog
    MAC limit reached: no, threshold: 75%
    MAC port down flush: enabled
    MAC Secure: disabled, Logging: disabled
    Split Horizon Group: none
    E-Tree: Root
    Dynamic ARP Inspection: disabled, Logging: disabled
    IP Source Guard: disabled, Logging: disabled
    DHCPv4 Snooping: disabled
    DHCPv4 Snooping profile: none
    IGMP Snooping: disabled
    IGMP Snooping profile: none
    MLD Snooping profile: none
    Storm Control: bridge-domain policer
    Static MAC addresses:
    Statistics:
      packets: received 221328661592 (multicast 0, broadcast 0, unknown unicast 0, unicast
0), sent 4516080000
      bytes: received 24346154850336 (multicast 0, broadcast 0, unknown unicast 0, unicast
0), sent 559962777746
      MAC move: 0
    Storm control drop counters:
      packets: broadcast 0, multicast 0, unknown unicast 0
      bytes: broadcast 0, multicast 0, unknown unicast 0
    Dynamic ARP inspection drop counters:
      packets: 0, bytes: 0
    IP source guard drop counters:
      packets: 0, bytes: 0
    PD System Data: AF-LIF-IPv4: 0x00013806 AF-LIF-IPv6: 0x00013807

List of Access PWs:
  PW: neighbor 192.127.0.1, PW ID 1, state is up ( established )
    PW class mpls, XC ID 0xc0000001 .
    Encapsulation MPLS, protocol LDP
    Source address 8.8.8.8
    PW type Ethernet, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
    LSP : Up

```

Flow Label flags configured (Tx=1,Rx=1), negotiated (Tx=0,Rx=0)

PW Status TLV in use		
MPLS	Local	Remote
Label	24007	24000
Group ID	0x1	0x1
Interface	Access PW	1
MTU	9086	9086
Control word	enabled	enabled
PW type	Ethernet	Ethernet
VCCV CV type	0x2	0x2
	(LSP ping verification)	(LSP ping verification)
VCCV CC type	0x7	0x7
	(control word)	(control word)
	(router alert label)	(router alert label)
	(TTL expiry)	(TTL expiry)

Incoming Status (PW Status TLV):

Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225473
Create time: 22/09/2019 15:00:09 (2w5d ago)
Last time status changed: 26/09/2019 11:17:06 (2w1d ago)
MAC withdraw messages: sent 3, received 0
Forward-class: 0
Static MAC addresses:
Statistics:
 packets: received 0 (unicast 0), sent 0
 bytes: received 0 (unicast 0), sent 0
 MAC move: 0
Storm control drop counters:
 packets: broadcast 0, multicast 0, unknown unicast 0
 bytes: broadcast 0, multicast 0, unknown unicast 0
MAC learning: enabled
Flooding:
 Broadcast & Multicast: enabled
 Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 64000, Action: none, Notification: syslog
MAC limit reached: no, threshold: 75%
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
E-Tree: Root
DHCPv4 Snooping: disabled
DHCPv4 Snooping profile: none
IGMP Snooping: disabled
IGMP Snooping profile: none
MLD Snooping profile: none
Storm Control: bridge-domain policer
List of VFIs:
List of Access VFIs:

Verify the status of BVI outgoing interface and collect the FGID using the **show mrrib vrf vrf1000 route** command:

```
RP/0/RP0/CPU0: # show mrrib vrf vrf1000 route 232.1.1.1 detail
```

```
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
```

```

CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
LD - Local Disinterest, DI - Decapsulation Interface
EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface
IRMI - IR MDT Interface

(87.2.1.2,232.1.1.1) Ver: 0xa5b9 RPF nbr: 87.2.1.2 Flags: RPF, FGID: 24312, Statistics
enabled: 0x3
Up: 00:13:05
Incoming Interface List
TenGigE0/0/0/0.2 Flags: A, Up: 00:13:05
Outgoing Interface List
BVI1 Flags: F NS LI, Up: 00:13:05

```

Multicast Label Distribution Protocol (MLDP) for Core

Multicast Label Distribution Protocol (MLDP) provides extensions to the Label Distribution Protocol (LDP) for the setup of point-to-multipoint (P2MP) and multipoint-to-multipoint (MP2MP) Label Switched Paths (LSPs) in Multiprotocol Label Switching (MPLS) networks.

MLDP eliminates the use of native multicast PIM to transport multicast packets across the core. In MLDP multicast traffic is label switched across the core. This saves a lot of control plane processing effort.

Characteristics of MLDP Profiles on Core

The following MLDP profiles are supported when the router is configured as a core router:

- Profile 5—Partitioned MDT - MLDP P2MP - BGP-AD - PIM C-mcast Signaling
- Profile 6—VRF MLDP - In-band Signaling
- Profile 7—Global MLDP In-band Signaling
- Profile 12—Default MDT - MLDP - P2MP - BGP-AD - BGP C-mcast Signaling
- Profile 17—Default MDT - MLDP - P2MP - BGP-AD - PIM C-mcast Signaling

Point-to-Multipoint Profiles on Core and Edge Routers

The following profiles are supported when the router is configured as a core router and edge router for p2mp:

- Profile 8—Global P2MP-TE
- Profile 10—VRF Static-P2MP-TE with BGP AD

Multicast MLDP Profile 14 support on an Edge Router

Table 2: Feature History Table

The MLDP Profile 14 is supported when the router is configured as an edge router.

IP based transport network is a cost efficient and convenient alternative to deliver video services combined with the delivery of other IP based services. To deliver IPTV content MLDP Profile 14 also called as the partitioned MDT, is supported when a router is configured as an edge router.

These are the characteristics of the profile 14:

- Customer traffic is SSM.
- Inter-AS Option A, B and C is supported.
- All PEs must have a unique BGP Route Distinguisher (RD) value.

Configuration Example for mLDP Profile 14 on Edge Routers

```
vrf one
 address-family ipv4 unicast
   import route-target
     1:1
   !
   export route-target
     1:1
   !
   !

router pim
 vrf one
  address-family ipv4
   rpf topology route-policy rpf-for-one
   mdt c-multicast-routing bgp
   !
   interface GigabitEthernet0/1/0/0
    enable
   !
  !
 !
 !

route-policy rpf-for-one
 set core-tree mldp-partitioned-p2mp
end-policy
!

multicast-routing
 vrf one
  address-family ipv4
   mdt source Loopback0
   mdt partitioned mldp ipv4 p2mp
   rate-per-route
  interface all enable
  bgp auto-discovery mldp
  !
  accounting per-prefix
 !
```



```

!
!
mpls ldp
 mldp
  logging notifications
  address-family ipv4
!
!
!

```

Configuration Example for MLDP on Core

```

mpls ldp
 mldp
  logging notifications
  address-family ipv4
!
!
!

```

Label Switched Multicast (LSM) Multicast Label Distribution Protocol (mLDP) based Multicast VPN (mVPN) Support

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

When router is positioned as the core router running mLDP, it only supports the Profiles 5, 6, 7, 12, 14, and 17 irrespective of the profiles supported on the edge router.

When router is positioned as the edge router running mLDP, it only supports the Profiles 6 and 7.



Note IPv6 is not supported for profile 10. Also IPv4 SM is not supported for mLDP profiles on an edge router.

For more information about the characteristics of each of the mLDP Profiles, [Characteristics of mLDP Profiles on Core](#)

Benefits of LSM mLDP based MVPN

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

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

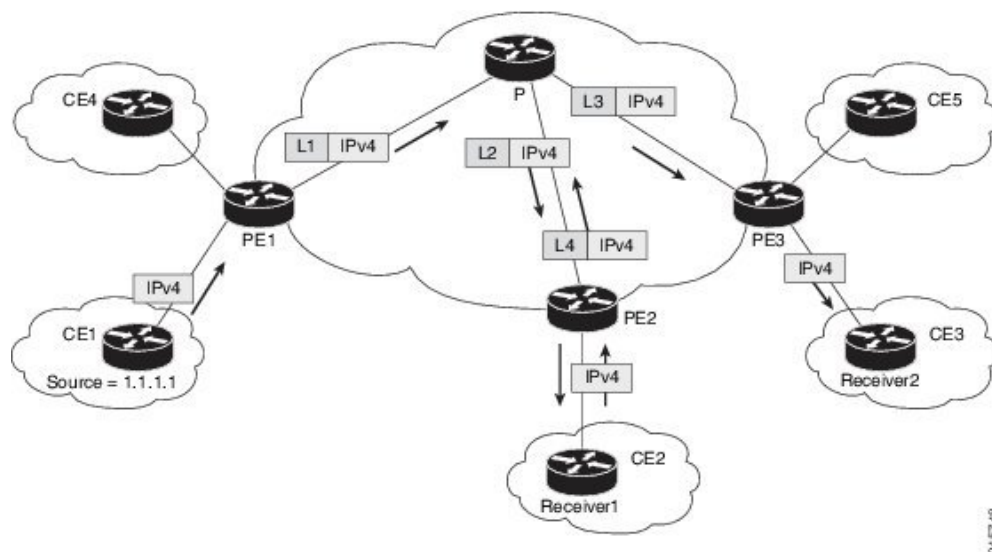
Configuring MLDP MVPN

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



Note When a Cisco NCS540 series Router is positioned as terminal node, it drops the IPv6 traffic that it receives from Cisco ASR 9000 Series Routers which is acting as a head node since EXP NULL label is sent at the Bottom of stack (BOS) over MLDP tunnel for IPV6 traffic.

Figure 5: MLDP based MPLS Network



Packet Flow in mLDP-based Multicast VPN

For each packet coming in, MPLS creates multiple out-labels. Packets from the source network are replicated along the path to the receiver network. The CE1 router sends out the native IP multicast traffic. The Provider Edge1 (PE1) router imposes a label on the incoming multicast packet and replicates the labeled packet towards the MPLS core network. When the packet reaches the core router (P), the packet is replicated with the appropriate labels for the MP2MP default MDT or the P2MP data MDT and transported to all the egress PEs. Once the packet reaches the egress PE, the label is removed and the IP multicast packet is replicated onto the VRF interface.

Realizing a mLDP-based Multicast VPN

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

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

The router performs the following important functions for the implementation of MLDP:

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

Configuration Process for MLDP MVPN (Intranet)

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

- Enabling MPLS MLDP
 - configure
 - mpls ldp mldp
- Configuring a VRF entry
 - configure
 - vrf *vrf_name*
 - address-family ipv4/ipv6 unicast
 - import route-target route-target-ext-community
 - export route-target route-target-ext-community
- Configuring VPN ID
 - configure
 - vrf *vrf_name*
 - vpn id *vpn_id*
- Configuring MVPN Routing and Forwarding instance
 - configure
 - multicast-routing vrf *vrf_name*
 - address-family ipv4
 - mdt default mldp ipv4 *root-node*
- Configuring the Route Distinguisher

- configure
- router bgp *AS Number*
- vrf *vrf_name*
- rd *rd_value*

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

- Configuring BGP MDT address family
 - configure
 - router bgp *AS Number*
 - address-family ipv4 mdt

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

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

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

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

- Configuring route-policy

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



Note The configuration of the above procedures depends on the profile used for each configuration.

Configure VRF MLDP In-Band Signaling on Edge Routers

To configure VRF MLDP in-band signaling (Profile 6) on edge routers, you must complete the following tasks:

1. Assign a route policy in PIM to select a reverse-path forwarding (RPF) topology.
2. Configure route policy to set the Multicast Distribution Tree (MDT) type to MLDP inband.
3. Enable MLDP-inband signaling in multicast routing.
4. Enable MPLS for MLDP.

Configuration

```

/* Assign a route policy in PIM to select a reverse-path forwarding (RPF) topology */
RP/0/RP0/CPU0:router(config)#router pim
RP/0/RP0/CPU0:router(config-pim)#vrf one
RP/0/RP0/CPU0:router(config-pim-one)#address-family ipv4
RP/0/RP0/CPU0:router(config-pim-one-ipv4)#rpf topology route-policy rpf-vrf-one

/* Configure route policy to set the MDT type to MLDP inband */
RP/0/RP0/CPU0:router(config)#route-policy rpf-vrf-one
RP/0/RP0/CPU0:router(config-rpl)#set core-tree mldp-inband
RP/0/RP0/CPU0:router(config-rpl)#end-policy

/* Enable MLDP-inband signaling in multicast routing */
RP/0/RP0/CPU0:router(config)#multicast-routing
RP/0/RP0/CPU0:router(config-mcast)#vrf one
RP/0/RP0/CPU0:router(config-mcast-one)#address-family ipv4
RP/0/RP0/CPU0:router(config-mcast-one-ipv4)#mdt source loopback 0
RP/0/RP0/CPU0:router(config-mcast-one-ipv4)#mdt mldp in-band-signaling ipv4
RP/0/RP0/CPU0:router(config-mcast-one-ipv4)#interface all enable

/* Enable MPLS MLDP */
RP/0/RP0/CPU0:router(config)#mpls ldp
RP/0/RP0/CPU0:router(config-ldp)#mldp

```

Configure Global MLDP In-band Signaling on Edge Routers

To configure global MLDP in-band signaling (Profile 7) on edge routers, you must complete the following tasks:

1. Assign a route policy in PIM to select a reverse-path forwarding (RPF) topology.
2. Configure route policy to set the MDT type to MLDP Inband.
3. Enable MLDP inband signaling in multicast routing.
4. Enable MPLS MLDP.

Configuration

```
/* Assign a route policy in PIM to select a reverse-path forwarding (RPF) topology */
RP/0/RP0/CPU0:router(config)#router pim
RP/0/RP0/CPU0:router(config-pim)#address-family ipv4
RP/0/RP0/CPU0:router(config-pim-default-ipv4)#rpf topology route-policy rpf-global
RP/0/RP0/CPU0:router(config-pim-default-ipv4)#interface TenGigE 0/11/0/1
RP/0/RP0/CPU0:router(config-pim-ipv4-if)#enable

/* Configure route policy to set the MDT type to MLDP inband */
RP/0/RP0/CPU0:router(config)#route-policy rpf-global
RP/0/RP0/CPU0:router(config-rpl)#set core-tree mldp-inband
RP/0/RP0/CPU0:router(config-rpl)#end-policy

/* Enable MLDP-inband signaling in multicast routing */
RP/0/RP0/CPU0:router(config)#multicast-routing
RP/0/RP0/CPU0:router(config-mcast)#address-family ipv4
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)#interface loopback 0
RP/0/RP0/CPU0:router(config-mcast-default-ipv4-if)#enable
RP/0/RP0/CPU0:router(config-mcast-default-ipv4-if)#exit
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)#mdt source loopback 0
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)#mdt mldp in-band-signaling ipv4
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)#interface all enable

/* Enable MPLS MLDP */
RP/0/RP0/CPU0:router(config)#mpls ldp
RP/0/RP0/CPU0:router(config-ldp)#mldp
```

Configuration Examples for MVPN Profiles

This section provides profile-wise configuration examples for the various MVPN profiles.

Configuration Examples for Inband mLDP Profiles

Profile-6: VRF Inband mLDP

```
router bgp 100
  mvpn
  !
  multicast-routing
```

```

vrf v61
address-family ipv4
  mdt source Loopback0
  mdt mtu 1600
  mdt mldp in-band-signaling ipv4
  interface all enable
!
address-family ipv6
  mdt mtu 1600
  mdt mldp in-band-signaling ipv4
  interface all enable
!
!
router pim
vrf v61
  address-family ipv4
    rpf topology route-policy mldp-inband
  !
  address-family ipv6
    rpf topology route-policy mldp-inband
  !
!
route-policy mldp-inband
  set core-tree mldp-inband
end-policy
!

```

Profile-7: Global Inband mLDP

```

multicast-routing
address-family ipv4
  mdt source Loopback0
  mdt mldp in-band-signaling ipv4
  ssm range Global-SSM-Group
  interface all enable
!
address-family ipv6
  mdt source Loopback0
  mdt mldp in-band-signaling ipv4
  ssm range Global-SSM-Group-V6
  interface all enable
!
router pim
  address-family ipv4
    rpf topology route-policy mldp-inband
  !
  address-family ipv6
    rpf topology route-policy mldp-inband
  !
!
route-policy mldp-inband
  set core-tree mldp-inband
end-policy
!

```

Configuration Examples for Inband mLDP Profiles on Edge Routers

Running Configuration for VRF MLDP In-Band Signaling (Profile 6)

```

router pim
vrf one
address-family ipv4
  rpf topology route-policy rpf-vrf-one

  route-policy rpf-vrf-one
    set core-tree mldp-inband
  end-policy

multicast-routing
vrf one
address-family ipv4
  mdt source Loopback0
  mdt mldp in-band-signaling ipv4
  interface all enable

mpls ldp
mldp

```

Running Configuration for Global MLDP In-band Signaling (Profile 7)

```

router pim
address-family ipv4
  rpf topology route-policy rpf-global
  interface TenGigE0/11/0/1
  enable

route-policy rpf-global
  set core-tree mldp-inband
end-policy

multicast-routing
address-family ipv4
  interface Loopback0
  enable
!
  mdt source Loopback0
  mdt mldp in-band-signaling ipv4
  interface all enable
!

mpls ldp
mldp

```

Verification of MLDP Configuration on Edge Routers

Use the following commands to verify the MLDP configuration on edge routers.

To check the MLDP neighbors, use the **show mpls mldp neighbor** command.

```

RP/0/RP0/CPU0:Head# show mpls mldp neighbors
mLDP neighbor database
MLDP peer ID      : 2.2.2.2:0, uptime 07:47:59 Up,
  Capabilities    : GR, Typed Wildcard FEC, P2MP, MP2MP
  Target Adj      : No
  Upstream count  : 1
  Branch count    : 1
  LDP GR          : Enabled
                  : Instance: 1
  Label map timer : never

```



```

Policy filter in :
Path count      : 1
Path(s)         : 12.1.1.2          TenGigE0/11/0/1 LDP
Adj list        : 12.1.1.2          TenGigE0/11/0/1
Peer addr list  : 2.25.32.2
                 : 2.2.2.2
                 : 11.1.1.1
                 : 12.1.1.2
                 : 13.10.1.1

```

To display the contents of the Label Information Base (LIB), use the **show mpls mldp bindings** command.

```

RP/0/RP0/CPU0:Head#show mpls mldp bindings
mLDP MPLS Bindings database

LSP-ID: 0x00001 Paths: 7 Flags:
0x00001 P2MP 5.5.5.5 [vpngv6 1:1 2015:1:1::3 ff3e::1]
  Local Label: 70009
  Remote Label: 64018 NH: 12.1.1.2 Inft: TenGigE0/11/0/1
  Remote Label: 64022 NH: 50.1.1.1 Inft: TenGigE0/11/0/1
  Remote Label: 30002 NH: 30.10.1.2 Inft: Bundle-Ether56
  Remote Label: 64023 NH: 60.1.1.2 Inft: HundredGigE0/0/1/1
  Remote Label: 64024 NH: 70.1.1.1 Inft: TenGigE0/11/0/2
  Remote Label: 64022 NH: 40.1.1.1 Inft: TenGigE0/11/0/3

```

To display the MLDP event traces, use the **show mpls mldp trace** command.

```

RP/0/RP0/CPU0:Head#show mpls mldp trace
3535 wrapping entries (631040 possible, 35584 allocated, 0 filtered, 3535 total)
May 30 23:30:21.121 MLDP GLO 0/RP0/CPU0 t6746 GEN : Trace pre-init iox success
May 30 23:30:21.121 MLDP GLO 0/RP0/CPU0 t6746 GEN : Debug pre-init iox success
May 30 23:30:21.121 MLDP GLO 0/RP0/CPU0 t6746 GEN : API pre-init iox success
May 30 23:30:21.121 MLDP GLO 0/RP0/CPU0 t6746 GEN : Bitfield pre-init iox success
May 31 12:08:39.465 MLDP GLO 0/RP0/CPU0 t6746 GEN : mldp_evm 0x563de8f01698 allocated
May 31 12:08:39.465 MLDP GLO 0/RP0/CPU0 t6746 GEN : EVM init iox success
May 31 12:08:39.472 MLDP GLO 0/RP0/CPU0 t6746 GEN : Registered EDM on active success
May 31 12:08:39.472 MLDP GLO 0/RP0/CPU0 t6746 GEN : EDM Ac/St init iox again
May 31 12:08:39.472 MLDP GLO 0/RP0/CPU0 t6746 GEN : Registered EDM Location on active
success
May 31 12:08:39.472 MLDP GLO 0/RP0/CPU0 t6746 GEN : EDM Loc init iox success
May 31 12:08:39.475 MLDP GLO 0/RP0/CPU0 t6746 GEN : LMRIB init iox success
May 31 12:08:39.475 MLDP GLO 0/RP0/CPU0 t18944 MRIB : MRIB connection established
May 31 12:08:39.475 MLDP GLO 0/RP0/CPU0 t6746 GEN : Interface manager init iox success
May 31 12:08:39.475 MLDP GLO 0/RP0/CPU0 t6746 GEN : Async init iox success
May 31 12:08:39.475 MLDP GLO 0/RP0/CPU0 t6746 GEN : Boolean init iox success
May 31 12:08:39.475 MLDP GLO 0/RP0/CPU0 t6746 GEN : Timers init iox success
May 31 12:08:39.479 MLDP GLO 0/RP0/CPU0 t6746 GEN : RUMP init iox success
May 31 12:08:39.479 MLDP GLO 0/RP0/CPU0 t6746 GEN : Chunks init iox success
May 31 12:08:39.509 MLDP ERR 0/RP0/CPU0 t6746 RIB : RIB not ready
May 31 12:08:39.509 MLDP ERR 0/RP0/CPU0 t6746 RIB : RIB not ready
May 31 12:08:39.512 MLDP GLO 0/RP0/CPU0 t6746 GEN : mldp_ens_event_ctx_chunk is NULL
May 31 12:08:39.512 MLDP GLO 0/RP0/CPU0 t6746 GEN : Context Table init iox success
May 31 12:08:39.512 MLDP GLO 0/RP0/CPU0 t6746 GEN : mldp_rib_main_evm 0x563de8fd23e8
allocated
May 31 12:08:39.512 MLDP GLO 0/RP0/CPU0 t6746 GEN : RIB Thread EVM init rib success
May 31 12:08:39.512 MLDP GLO 0/RP0/CPU0 t6746 GEN : RIB Thread Chunk init rib success
May 31 12:08:39.512 MLDP GLO 0/RP0/CPU0 t6746 GEN : RIB Thread queue init rib success
May 31 12:08:39.512 MLDP GLO 0/RP0/CPU0 t6746 RIB : Bound to RIB, fd: 354

```

