



# Implementing Multicast

- [Implementing Layer-3 Multicast Routing, on page 1](#)
- [Protocol Independent Multicast, on page 2](#)
- [PIM BFD Overview, on page 3](#)
- [Reverse Path Forwarding , on page 5](#)
- [PIM Bootstrap Router, on page 6](#)
- [PIM-Source Specific Multicast, on page 7](#)
- [Multicast Source Discovery Protocol, on page 10](#)
- [PIM-Sparse Mode, on page 15](#)
- [Internet Group Management Protocol, on page 17](#)
- [Use Case: Video Streaming, on page 20](#)

## 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.

NCS 5500 series router supports the following protocols 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 on NCS 5500 Series Router

- 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.

## 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
TenGigE0/0/0/3)
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 0/3/CPU0
Interface : FINT0/3/CPU0 (Enabled)
SW Mcast pkts in : 0, SW Mcast pkts out : 0
TTL Threshold : 0
Ref Count : 2
Interface : TenGigE0/3/0/0/0 (Enabled)
SW Mcast pkts in : 0, SW Mcast pkts out : 0
TTL Threshold : 0
Ref Count : 3
Interface : TenGigE0/3/0/9/0 (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
```

## 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.

NCS 5500 series router supports Protocol Independent Multicast in Source-Specific Multicast (PIM-SSM). 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

This section describes how you can configure PIM BFD

```
Router# configure
Router(config)# router pim address-family ipv4
Router(config-pim-default-ipv4)# interface HundredGige 0/1/0/1
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 TengigabitEthernet 0/0/0/4
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
Router(config-pim-default-ipv4)# interface TengigabitEthernet 0/0/0/4.101
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
Router(config-pim-default-ipv4)# interface Bundle-Ether 101
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
Router(config-pim-default-ipv4)# commit
```

### Running Configuration

```

router pim
address-family ipv4
interface HundredGige 0/1/0/1
  bfd minimum-interval 10
  bfd fast-detect
  bfd multiplier 3
!
interface TengigabitEthernet 0/0/0/4
  bfd minimum-interval 50
  bfd fast-detect
  bfd multiplier 3
!
interface TengigabitEthernet 0/0/0/4.101
  bfd minimum-interval 50
  bfd fast-detect
  bfd multiplier 3
!
interface Bundle-Ether 101
  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
-----
Hu0/0/1/3        10.12.12.2     0s (0s*0) 90ms (30ms*3)         UP          Yes
0/0/CPU0
Hu0/0/1/2        10.12.12.2     0s (0s*0) 90ms (30ms*3)         UP          Yes
0/0/CPU0
Hu0/0/1/1        10.18.18.2     0s (0s*0) 90ms (30ms*3)         UP          Yes
0/0/CPU0
Te0/0/0/4.101    10.112.112.2   0s (0s*0) 90ms (30ms*3)         UP          Yes
0/0/CPU0
BE101            10.18.18.2     n/a        n/a                    UP          No    n/a
BE102            10.12.12.2     n/a        n/a                    UP          No    n/a

```

```

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-if)#static-rpf 10.0.0.1 32 TenGigE 0/0/0/1 192.168.0.2
Router(config-ipv4-acl)#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
```

# 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
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
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.




---

**Note** PIM-SSM supports IPv6 from Cisco IOS XR Release 6.2.2

---

- 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 broad cast traffic. The source is provided by interested receivers through IGMPv3 membership reports.

## 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
```

Configures SSM service for the IPv6 address range defined by access list 6.

```
Router#config
Router(config)#ipv6 access-list 6
Router(config-ipv6-acl)#permit ipv6 any ff30:0:0:2::/32
Router(config-ipv6-acl)#exit
Router(config)#multicast-routing
Router(config-mcast)#address-family ipv6
Router(config-mcast-default-ipv6)#ssm range 6
Router(config-mcast-default-ipv6)#commit
Router(config-mcast-default-ipv6)#end
```

### Running Configuration

```
Router#show running multicast-routing
multicast-routing
  address-family ipv4
    ssm range 4
```



```

interface all enable
!

Router#show running multicast-routing
multicast-routing
address-family ipv6
  ssm range 6
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-ipv4)#dr-priority 2
Router(config-pim-default-ipv4)#spt-threshold infinity
Router(config-pim-default-ipv4)#interface TenGigE 0/0/0/1
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 TenGigE0/0/0/1
  dr-priority 4
  hello-interval 45
```

### Verification

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

```
Router#show pim interface te0/0/0/1
PIM interfaces in VRF default
Address          Interface          PIM  Nbr  Hello  DR      DR Count Intvl
  Prior
100.1.1.1        TenGigE0/0/0/1    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.

### MSDP Configuration Submode

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

## Interconnecting PIM-SM Domains with MSDP

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

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

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

**Before you begin**

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

**SUMMARY STEPS**

1. **configure**
2. **interface** *type interface-path-id*
3. **ipv4 address** *address mask*
4. **exit**
5. **router msdp**
6. **default-peer** *ip-address* [**prefix-list** *list*]
7. **originator-id** *type interface-path-id*
8. **peer** *peer-address*
9. **connect-source** *type interface-path-id*
10. **mesh-group** *name*
11. **remote-as** *as-number*
12. **commit**
13. **show msdp** [**ipv4**] **globals**
14. **show msdp** [**ipv4**] **peer** [*peer-address*]
15. **show msdp** [**ipv4**] **rpf** *rpf-address*

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b>	
<b>Step 2</b>	<b>interface</b> <i>type interface-path-id</i>  <b>Example:</b>  RP/0/RP0/CPU0:router(config)# interface loopback 0	(Optional) Enters interface configuration mode to define the IPv4 address for the interface.  <b>Note</b> This step is required if you specify an interface type and number whose primary address becomes the source IP address for the TCP connection.
<b>Step 3</b>	<b>ipv4 address</b> <i>address mask</i>  <b>Example:</b>  RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.0.1.3 255.255.255.0	(Optional) Defines the IPv4 address for the interface.  <b>Note</b> 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 <b>connect-source</b> command.
<b>Step 4</b>	<b>exit</b>  <b>Example:</b>  RP/0/RP0/CPU0:router(config-if)# end	Exits interface configuration mode.

	Command or Action	Purpose
<b>Step 5</b>	<b>router msdp</b> <b>Example:</b> RP/0/RP0/CPU0:router(config)# router msdp	Enters MSDP protocol configuration mode.
<b>Step 6</b>	<b>default-peer ip-address [prefix-list list]</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-msdp)# default-peer 172.23.16.0	(Optional) Defines a default peer from which to accept all MSDP SA messages.
<b>Step 7</b>	<b>originator-id type interface-path-id</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-msdp)# originator-id /1/1/0	(Optional) Allows an MSDP speaker that originates a (Source-Active) SA message to use the IP address of the interface as the RP address in the SA message.
<b>Step 8</b>	<b>peer peer-address</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-msdp)# peer 172.31.1.2	Enters MSDP peer configuration mode and configures an MSDP peer. <ul style="list-style-type: none"> <li>• Configure the router as a BGP neighbor.</li> <li>• 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.</li> </ul>
<b>Step 9</b>	<b>connect-source type interface-path-id</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-msdp-peer)# connect-source loopback 0	(Optional) Configures a source address used for an MSDP connection.
<b>Step 10</b>	<b>mesh-group name</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-msdp-peer)# mesh-group internal	(Optional) Configures an MSDP peer to be a member of a mesh group.
<b>Step 11</b>	<b>remote-as as-number</b> <b>Example:</b> RP/0/RP0/CPU0:router(config-msdp-peer)# remote-as 250	(Optional) Configures the remote autonomous system number of this peer.

	Command or Action	Purpose
Step 12	<b>commit</b>	
Step 13	<b>show msdp [ipv4] globals</b>  <b>Example:</b>  RP/0/RP0/CPU0:router# show msdp globals	Displays the MSDP global variables.
Step 14	<b>show msdp [ipv4] peer [peer-address]</b>  <b>Example:</b>  RP/0/RP0/CPU0:router# show msdp peer 172.31.1.2	Displays information about the MSDP peer.
Step 15	<b>show msdp [ipv4] rpf rpf-address</b>  <b>Example:</b>  RP/0/RP0/CPU0:router# show msdp rpf 172.16.10.13	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.

## SUMMARY STEPS

1. **configure**
2. **router msdp**
3. **sa-filter** {in | out} {ip-address | peer-name} [**list** access-list-name] [**rp-list** access-list-name]
4. **cache-sa-state** [**list** access-list-name] [**rp-list** access-list-name]
5. **ttl-threshold** ttl-value
6. **exit**
7. **ipv4 access-list** name [sequence-number] **permit** source [source-wildcard]
8. **commit**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure</b>	
<b>Step 2</b>	<b>router msdp</b>  <b>Example:</b>  RP/0/RP0/CPU0:router(config)# router msdp	Enters MSDP protocol configuration mode.
<b>Step 3</b>	<b>sa-filter</b> {in   out} {ip-address   peer-name} [ <b>list</b> access-list-name] [ <b>rp-list</b> access-list-name]  <b>Example:</b>  RP/0/RP0/CPU0:router(config-msdp)# sa-filter out router.cisco.com list 100	Configures an incoming or outgoing filter list for messages received from the specified MSDP peer. <ul style="list-style-type: none"> <li>• If you specify both the <b>list</b> and <b>rp-list</b> keywords, all conditions must be true to pass any source, group (S, G) pairs in outgoing Source-Active (SA) messages.</li> <li>• You must configure the <b>ipv4 access-list</b> command in <a href="#">Step 7, on page 15</a>.</li> <li>• If all match criteria are true, a <b>permit</b> from the route map passes routes through the filter. A <b>deny</b> filters routes.</li> <li>• This example allows only (S, G) pairs that pass access list 100 to be forwarded in an SA message to the peer named router.cisco.com.</li> </ul>
<b>Step 4</b>	<b>cache-sa-state</b> [ <b>list</b> access-list-name] [ <b>rp-list</b> access-list-name]  <b>Example:</b>  RP/0/RP0/CPU0:router(config-msdp)# cache-sa-state 100	Creates and caches source/group pairs from received Source-Active (SA) messages and controls pairs through access lists.
<b>Step 5</b>	<b>ttl-threshold</b> ttl-value  <b>Example:</b>	(Optional) Limits which multicast data is sent in SA messages to an MSDP peer.

	Command or Action	Purpose
	<pre>RP/0/RP0/CPU0:router(config-msdp)# ttl-threshold 8</pre>	<ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• This example configures a TTL threshold of eight hops.</li> </ul>
<b>Step 6</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-msdp)# exit</pre>	Exits the current configuration mode.
<b>Step 7</b>	<p><b>ipv4 access-list name [sequence-number] permit source [source-wildcard]</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config)# ipv4 access-list 100 20 permit 239.1.1.1 0.0.0.0</pre>	<p>Defines an IPv4 access list to be used by SA filtering.</p> <ul style="list-style-type: none"> <li>• In this example, the access list 100 permits multicast group 239.1.1.1.</li> <li>• The <b>ipv4 access-list</b> command is required if the keyword <b>list</b> is configured for SA filtering in <a href="#">Step 3</a>, on page 14.</li> </ul>
<b>Step 8</b>	<b>commit</b>	

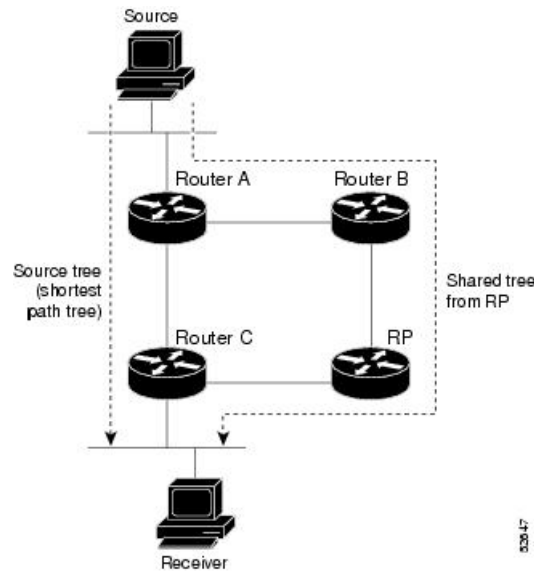
## PIM-Sparse Mode

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).

---

## 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.

NCS 5500 supports IGMPv3 by default. No configuration is required. IGMP Version 3 permits joins and leaves for certain source and group pairs instead of requesting traffic from all sources in the multicast group.

---

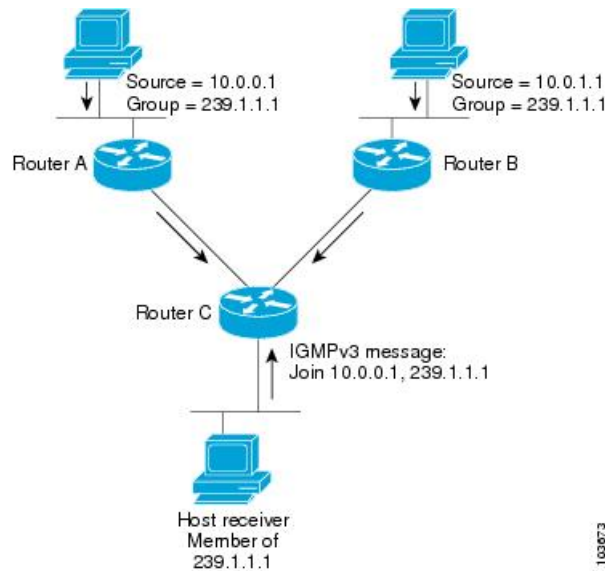
### Functioning of IGMP Routing

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 2: IGMP Signaling



## Configuring IGMP Per Interface States 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 0/0/0/6, which is set to 3000:

```
Router#config
Router(config)#router igmp
Router(config-igmp)#maximum groups-per-interface 4000
Router(config-igmp)#interface TenGigE 0/0/0/6
Router(config-igmp-default-if)#maximum groups-per-interface 3000
Router(config-igmp-default-if)#commit
```

### Running Configuration

```
router igmp
 interface TenGigE0/0/0/6
  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
TenGigE0/0/0/0            5       4000
TenGigE0/0/0/1            5       4000
TenGigE0/0/0/2            0       4000
TenGigE0/0/0/3            5       4000
TenGigE0/0/0/6            5       3000
TenGigE0/0/0/18           5       4000
TenGigE0/0/0/19           5       4000
TenGigE0/0/0/6.1          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)#int te0/0/0/3
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 TenGigE0/0/0/3
 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
TenGigE0/0/0/3 Flags: F NS LI, Up: 00:01:11

```

## Use Case: Video Streaming

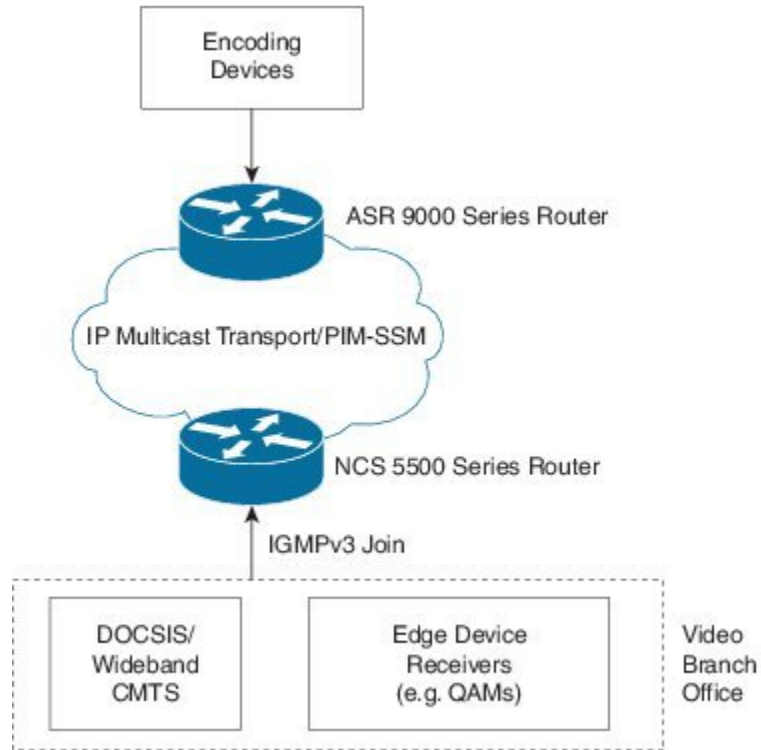
In today's broadcast video networks, proprietary transport systems are used to deliver entire channel line-ups to each video branch office. IP based transport network would be a cost efficient/convenient alternative to deliver video services combined with the delivery of other IP based services. (Internet 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 master 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 master 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 3: Video Streaming



365808

