



# Configuring Multicast Source Discovery Protocol

---

This chapter describes the Multicast Source Discovery Protocol (MSDP) feature. For a complete description of the MSDP commands in this chapter, refer to the “Multicast Source Discovery Protocol Commands” chapter of the *Cisco IOS IP and IP Routing Command Reference* publication. To locate documentation of other commands in this chapter, use the command reference master index or search online.

MSDP is a mechanism to connect multiple Protocol-Independent Multicast (PIM) sparse-mode domains. MSDP allows multicast sources for a group to be known to all rendezvous point(s) (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains. An RP runs MSDP over TCP to discover multicast sources in other domains.

An RP in a PIM sparse-mode domain has an MSDP peering relationship with MSDP-enabled routers in another domain. The peering relationship occurs over a TCP connection, where primarily a list of sources sending to multicast groups is exchanged. The TCP connections between RPs are achieved by the underlying routing system. The receiving RP uses the source lists to establish a source path.

The purpose of this topology is to have domains discover multicast sources in other domains. If the multicast sources are of interest to a domain that has receivers, multicast data is delivered over the normal, source-tree building mechanism in PIM-SM.

MSDP is also used to announce sources sending to a group. These announcements must originate at the domain’s RP.

MSDP depends heavily on BGP or MBGP for interdomain operation. We recommend that you run MSDP in RPs in your domain that are RPs for sources sending to global groups to be announced to the internet.

## How MSDP Works

Figure 62 illustrates MSDP operating between two MSDP peers. PIM uses MSDP as the standard mechanism to register a source with the RP of a domain.

When MSDP is configured, the following sequence occurs. When a source’s first data packet is registered by the first-hop router, that same data packet is decapsulated by the RP and forwarded down the shared tree. That packet is also reencapsulated in a Source-Active (SA) message that is immediately forwarded to all MSDP peers. The SA message identifies the source, the group the source is sending to, and the RP’s own address or the originator ID, if configured. If the peer is an RP and has a member of that multicast group, the data packet is decapsulated and forwarded down the shared-tree in the remote domain.

The PIM designated router (DR) directly connected to the source sends the data encapsulated in a PIM Register message to the RP in the domain.

**Note**

---

Note that this happens only once per source, when the source goes active. If the source times out, this process happens again when it goes active again. This is different from the periodic SA message that contains all sources that are registered to the originating RP. These messages have no data.

---

Each MSDP peer receives and forwards the SA message away from the originating RP to achieve *peer-RPF flooding*. The concept of peer-RPF flooding is with respect to forwarding SA messages. The router examines the BGP or MBGP routing table to determine which peer is the next hop toward the originating RP of the SA message. Such a peer is called an “RPF peer” (Reverse-Path Forwarding peer). The router forwards the message to all MSDP peers other than the RPF peer.

If the MSDP peer receives the same SA message from a non-RPF peer toward the originating RP, it drops the message. Otherwise, it forwards the message on to all its MSDP peers.

When an RP for a domain receives an SA message from an MSDP peer, it determines if it has any group members interested in the group the SA message describes. If the (\*, G) entry exists with a nonempty outgoing interface list, the domain is interested in the group, and the RP triggers an (S, G) join toward the source.

**Figure 62** *MSDP Running Between RP Peers*

## Benefits

MSDP has the following benefits:

- It breaks up the shared multicast distribution tree. You can make the shared tree local to your domain. Your local members join the local tree, and Join messages for the shared tree never need to leave your domain.
- PIM sparse-mode domains can rely on their own RPs only, thus decreasing reliance on RPs in another domain. This increases security because you can prevent your sources from being known outside your domain.
- Domains with only receivers can receive data without globally advertising group membership.
- Global source multicast routing table state is not required, thus saving on memory.

## Prerequisites

Before configuring MSDP, the addresses of all MSDP peers must be known in BGP or MBGP. If that does not occur, you must configure MSDP default peering when you configure MSDP.

## MSDP Configuration Tasks

To configure an MSDP peer and various MSDP options, perform the following tasks. The first task is required; the remaining are optional.

- Configuring an MSDP Peer (Required)
- Caching Source-Active State (Optional)
- Requesting Source Information from an MSDP Peer (Optional)
- Controlling Source Information That Your Router Originates (Optional)
- Controlling Source Information That Your Router Forwards (Optional)
- Controlling Source Information That Your Router Receives (Optional)
- Configuring a Default MSDP Peer (Optional)
- Configuring an MSDP Mesh Group (Optional)
- Shutting Down an MSDP Peer (Optional)
- Including a Bordering PIM Dense-Mode Region in MSDP (Optional)
- Configuring an Originating Address Other Than the RP Address (Optional)

See the section “MSDP Configuration Examples” at end of this chapter for configuration examples.

## Configuring an MSDP Peer

You enable MSDP by configuring an MSDP peer to the local router.



### Note

The router you specify by Domain Naming System (DNS) name or IP address as an MSDP peer is probably a BGP neighbor. If it is not, see the section “Configuring a Default MSDP Peer” later in this document.

To configure an MSDP peer, use the following commands in global configuration mode. The second command is optional.

Command	Purpose
<code>ip msdp peer {peer-name   peer-address}</code> <code>[connect-source type number] [remote-as as-number]</code>	Enables MSDP and configures an MSDP peer as specified by the DNS name or IP address.  If you specify the <b>connect-source</b> keyword, the primary address of the specified local interface <i>type</i> and <i>number</i> is used as the source IP address for the TCP connection. The <b>connect-source</b> keyword is recommended, especially for MSDP peers on a border that peer with a router inside the remote domain.
<code>ip msdp description {peer-name   peer-address} text</code>	Configures a description for a specified peer to make it easier to identify in a configuration or in <b>show</b> command output.

## Caching Source-Active State

By default, the router does not cache source/group pairs from received SA messages. Once the router forwards the MSDP Source-Active information, it does not store it in memory. Therefore, if a member joins a group soon after a Source-Active message is received by the local RP, that member will need to wait until the next SA message to hear about the source. This delay is known as join latency.

If you want to sacrifice some memory in exchange for reducing the latency of the source information, you can configure the router to cache Source-Active messages. To have the router cache source/group pairs, use the following command in global configuration mode:

Command	Purpose
<code>ip msdp cache-sa-state [list access-list-number]</code>	Creates SA state (cache source/group pairs). Those pairs that pass the access list are cached.

An alternative to caching the SA state is to request source information from a peer, which is described in the following section, “Requesting Source Information from an MSDP Peer.” If you cache the information, you need not trigger a request for it.

## Requesting Source Information from an MSDP Peer

Local RPs can send Source-Active Requests and get immediate response for all active sources for a given group. By default, the router does not send any Source-Active Request messages to its MSDP peers when a new member joins a group and wants to receive multicast traffic. The new member just waits to receive the next periodic Source-Active message.

If you want a new member of a group to learn the current, active multicast sources in a connected PIM sparse-mode domain that are sending to a group, configure the router to send Source-Active Request messages to the specified MSDP peer when a new member joins a group. Doing so reduces join latency, but requires some memory.

Note that information can be requested only from caching peers.

To configure this feature, use the following command in global configuration mode:

Command	Purpose
<code>ip msdp sa-request {ip-address   name}</code>	Configures the router to send Source-Active Request messages to the specified MSDP peer when a receiver becomes active, so the receiver can learn about multicast sources in a group. The peer replies with the information it is SA cache. If the peer does not have a cache configured, this command provides nothing.

Repeat the preceding command for each MSDP peer that you want to supply you with Source-Active messages.

An alternative to requesting source information is to cache the source-active state, which is described in the earlier section “Caching Source-Active State.” If you cache the information, you need not trigger a request for it.

## Controlling Source Information That Your Router Originates

There are two ways to control the multicast source information that originates with your router. You can control the following:

- Which sources you will advertise (based on your sources)
- Whom you will provide source information to (based on knowing who is asking you for information)

To control which sources you will advertise, see the following section, “Redistributing Sources.” To control whom you will provide source information to, see the section “Controlling Source Information That Your Router Forwards” later in this chapter.

## Redistributing Sources

Source-Active messages are originated on RPs to which sources have registered. By default, any source that registers with an RP will be advertised. The “A flag” is set in the RP when a source is registered. This means the source will be advertised in an SA unless it is filtered with the following command.

To further restrict which registered sources are advertised, use the following command in global configuration mode. The access list or autonomous system path access list determines which (S, G) pairs are advertised.

Command	Purpose
<code>ip msdp redistribute [list access-list-name] [asn aspath-access-list-number] [route-map map]</code>	Advertises (S, G) pairs that pass the access list or route map to other domains.

**Note**

The `ip msdp redistribute` command could also be used to advertise sources that are known to the RP but not registered. However, we strongly recommend that you NOT originate advertisements for sources that have not registered with the RP.

## Filtering Source-Active Request Messages

By default, only routers that are caching Source-Active information can respond to Source-Active Requests. By default, such a router honors all Source-Active Request messages from its MSDP peers. That is, it will supply the IP addresses of the sources that are active.

However, you can configure the router to ignore all Source-Active Requests from an MSDP peer. Or, you can honor only those Source-Active Request messages from a peer for groups described by a standard access list. If the access list passes, Source-Active Request messages will be accepted. All other such messages from the peer for other groups will be ignored.

To configure one of these options, use the appropriate command in global configuration mode:

Command	Purpose
<code>ip msdp filter-sa-request ip-address   name</code>	Filters all Source-Active Request messages from the specified MSDP peer.
<code>ip msdp filter-sa-request ip-address   name list access-list-number</code>	Filters Source-Active Request messages from the specified MSDP peer for groups that pass the standard access list. The access list describes a multicast group address.

## Controlling Source Information That Your Router Forwards

By default, the router forwards all Source-Active messages it receives to all of its MSDP peers. However, you can prevent outgoing messages from being forwarded to a peer by using a filter or by setting a time to live (TTL). These methods are described in the following sections.

### Using a Filter

By creating a filter, you can do one of 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

To apply a filter, use one of the following commands in global configuration mode:

Command	Purpose
<code>ip msdp sa-filter out {ip-address   name}</code>	Filters all Source-Active messages to the specified MSDP peer.
<code>ip msdp sa-filter out {ip-address   name} list access-list-name</code>	To the specified MSDP peer, passes only those Source-Active messages that pass the extended access list. If both the <b>list</b> and the <b>route-map</b> keywords are used, all conditions must be true to pass any (S, G) pair in outgoing SA messages.
<code>ip msdp sa-filter out {ip-address   name} route-map map-tag</code>	To the specified MSDP peer, passes only those Source-Active messages that meet the match criteria in the route map <i>map-tag</i> . If all match criteria are true, a <b>permit</b> from the route map will pass routes through the filter. A <b>deny</b> will filter routes. If both the <b>list</b> and the <b>route-map</b> keywords are used, all conditions must be true to pass any (S, G) in outgoing SA messages.

## Using TTL to Limit the Multicast Data Sent in SA Messages

You can use TTL to control what data will be encapsulated in the first SA message for every source. For example, you could limit internal traffic to a TTL of 8. If you want other groups to go to external locations, you would have to send those packets with a TTL greater than 8.

To establish a TTL threshold, use the following command in global configuration mode:

Command	Purpose
<code>ip msdp ttl-threshold {ip-address   name} ttl</code>	Limits which multicast data will be encapsulated in the first Source-Active message to the specified MSDP peer.

## Controlling Source Information That Your Router Receives

By default, the router receives all Source-Active messages its MSDP Reverse-Path Forwarding peers send to it. However, you can control the source information you receive from MSDP peers by filtering incoming Source-Active messages. In other words, you can configure the router not to accept them.

You can do one of the following:

- Filter all incoming Source-Active 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

To apply a filter, use one of the following commands in global configuration mode:

Command	Purpose
<code>ip msdp sa-filter in ip-address   name</code>	From the specified MSDP peer, filters all Source-Active messages received.
<code>ip msdp sa-filter in ip-address   name list access-list-name</code>	From the specified MSDP peer, passes incoming Source-Active messages that pass the extended access list.  If both the <b>list</b> and the <b>route-map</b> keywords are used, all conditions must be true to pass any (S, G) pair in incoming SA messages.
<code>ip msdp sa-filter in ip-address   name route-map map-tag</code>	From the specified MSDP peer, passes only those Source-Active messages that meet the match criteria in the route-map <i>map-tag</i> .  If all match criteria are true, a <b>permit</b> from the route map will pass routes through the filter. A <b>deny</b> will filter routes.  If both the <b>list</b> and the <b>route-map</b> keywords are used, all conditions must be true to pass any (S, G) in incoming SA messages.

## Configuring a Default MSDP Peer

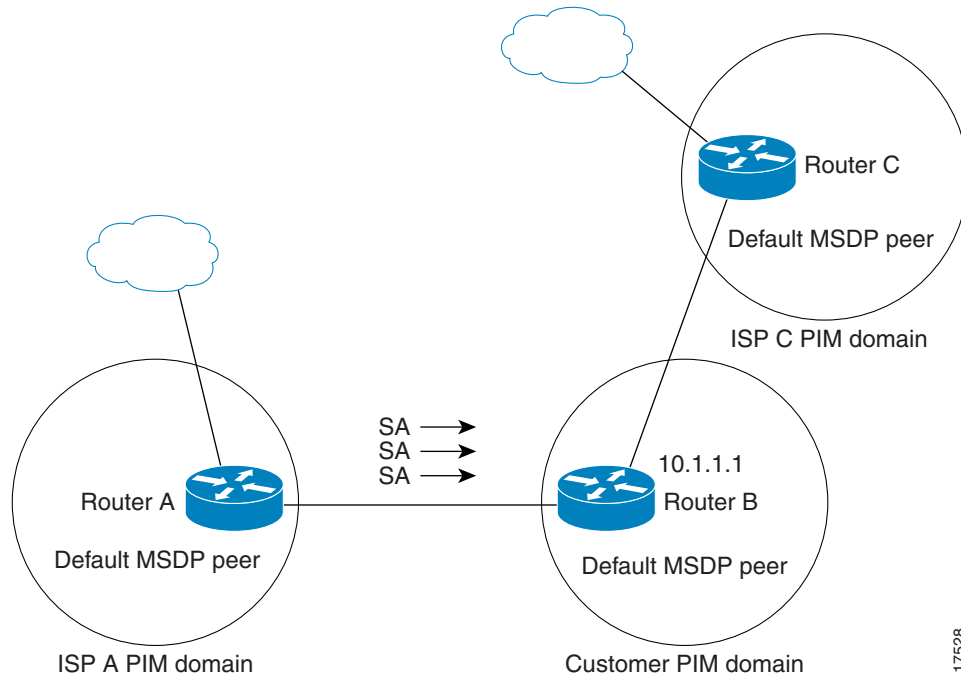
An MSDP peer of the local router is probably a BGP peer also. However, if you do not want to have or cannot have a BGP peer, you could define a default MSDP peer from which to accept all SA messages. The default MSDP peer must be a previously configured MSDP peer. Configure a default MSDP peer when you are not BGP- or MBGP-peering with an MSDP peer. If a single MSDP peer is configured, a router will always accept all SA messages sent to it from that peer.

Figure 63 illustrates a scenario where default MSDP peers might be used. In the figure, a customer who owns Router B is connected to the internet via two Internet Service Providers (ISPs), one who owns Router A and the other who owns Router C. They are not running BGP or MBGP between them. In order for the customer to learn about sources in the ISP's domain or in other domains, Router B identifies Router A as its default MSDP peer. Router B advertises SA messages to both Router A and Router C, but accepts SA messages either from Router A only or Router C only. If Router A is first in the configuration file, it will be used if it is up and running. If Router A is not running, then and only then will Router B accept SA messages from Router C.

The ISP will also likely use a prefix list to define which prefixes it will accept from the customer's router. The customer will define multiple default peers, each having one or more prefixes associated with it.

The customer has two ISPs to use. He defines both ISPs as default peers. As long as the first default peer identified in the configuration is up and running, it will be the default peer and the customer will accept all SA messages it receives from that peer.

Figure 63 Default MSDP Peer Scenario



Router B advertises SAs to Router A and Router C, but uses only Router A or Router C to accept SA messages. If Router A is first in the configuration file, it will be used if it is up and running. If Router A is not running, then and only then will Router B accept SAs from Router C. This is the behavior without a prefix list.

If you specify a prefix list, the peer will be a default peer only for the prefixes in the list. You can have multiple active default peers when you have a prefix list associated with each. When you do not have any prefix lists, you can configure multiple default peers, but only the first one is the active default peer as long as the router has connectivity to this peer and the peer is alive. If the first configured peer goes down or the connectivity to this peer goes down, the second configured peer becomes the active default, and so on.

To specify a default MSDP peer, use the following command in global configuration mode:

Command	Purpose
<code>ip msdp default-peer ip-address   name [prefix-list list]</code>	Defines a default MSDP peer.

See the section “Default MSDP Peer” at the end of this chapter for a sample configuration.

## Configuring an MSDP Mesh Group

An MSDP mesh group is a group of MSDP speakers that have fully meshed MSDP connectivity between one another. Any SA messages received from a peer in a mesh group are not forwarded to other peers in the same mesh group. Thus, you reduce SA message flooding and simplify peer-RPF flooding. The following command is used when there are multiple RPs within a domain. It is especially used to send SA messages across a domain.

## Shutting Down an MSDP Peer

You can configure multiple mesh groups (with different names) in a single router.

To create a mesh group, use the following command in global configuration mode for each MSDP peer in the group:

Command	Purpose
<code>ip msdp mesh-group name {ip-address   name}</code>	Configures an MSDP mesh group and indicates that an MSDP peer belongs to that mesh group.

## Shutting Down an MSDP Peer

If you want to configure many MSDP commands for the same peer and you do not want the peer to go active, you can shut down the peer, configure it, and later bring it up.

You might also want to shut down an MSDP session without losing configuration information for the peer.

When a peer is shut down, the TCP connection is terminated and not restarted.

To shut down a peer, use the following command in global configuration mode:

Command	Purpose
<code>ip msdp shutdown {peer-name   peer address}</code>	Administratively shuts down the specified MSDP peer.

## Including a Bordering PIM Dense-Mode Region in MSDP

You might have a router that borders a PIM sparse-mode region with a dense-mode region. By default, sources in the dense-mode region are not included in MSDP. You could configure this border router to send SA messages for sources active in the dense-mode region. If you do so, it is very important to also configure the `ip msdp redistribute` command to apply to only local sources. This can result in (S, G) state remaining long after a source in the dense-mode domain has stopped sending.



### Note

This command is not recommended. It is better to configure the border router in the sparse-mode domain to proxy-register sources in the dense-mode domain to the RP of the sparse-mode domain and have the sparse-mode domain use standard MSDP procedures to advertise these sources.

To configure the border router to send SA messages for sources active in the dense-mode region, use the following command in global configuration mode:

Command	Purpose
<code>ip msdp border sa-address type number</code>	Configures the router on the border between a dense-mode and sparse-mode region to send SA messages about active sources in the dense-mode region. The IP address of the interface is used as the Originator-ID, which is the RP field in the SA message.

## Configuring an Originating Address Other Than the RP Address

If you want to change the Originator ID for any reason, use the **ip msdp originator-id** command in this section. For example, you might change the Originator ID in one of these cases:

- If you configure a logical RP on multiple routers in an MSDP mesh group. For an example of a logical RP, see the section “Logical RP” later in this document.
- If you have a router that borders a PIM sparse-mode domain and a dense-mode domain. If a router borders a dense-mode domain for a site, and sparse-mode is being used externally, you might want dense-mode sources to be known to the outside world. Because this router is not an RP, it would not have an RP address to use in an SA message. Therefore, this command provides the RP address by specifying the address of the interface.

To allow an MSDP speaker that originates a Source-Active message to use its interface’s IP address as the RP address in the SA message, use the following command in global configuration mode:

Command	Purpose
<code>ip msdp originator-id type number</code>	Configures the RP address in SA messages to be the address of the originating router’s interface.

## Monitoring and Maintaining MSDP

To monitor MSDP Source-Active messages, peers, state, or peer status, use the following commands in EXEC mode:

Command	Purpose
<code>debug ip msdp [peer-address   name] [detail] [routes]</code>	Debugs an MSDP activity.
<code>debug ip msdp resets</code>	Debugs MSDP peer reset reasons.
<code>show ip msdp count [autonomous-system-number]</code>	Displays the number of sources and groups originated in SA messages from each autonomous system. The <b>ip msdp cache-sa-state</b> command must be configured for this command to produce any output.
<code>show ip msdp peer [peer-address   name]</code>	Displays detailed information about an MSDP peer.
<code>show ip msdp sa-cache [group-address   source-address] [group-name   source-name] [autonomous-system-number]</code>	Displays (S, G) state learned from MSDP peers.
<code>show ip msdp summary</code>	Displays MSDP peer status and SA message counts.

To clear MSDP connections, statistics, or SA cache entries, use the following commands in EXEC mode:

Command	Purpose
<code>clear ip msdp peer [peer-address   name]</code>	Clears the TCP connection to the specified MSDP peer, resetting all MSDP message counters.
<code>clear ip msdp statistics [peer-address   name]</code>	Clears the TCP connection to the specified MSDP peer, reset all MSDP message counters.
<code>clear ip msdp sa-cache [group-address   name]</code>	Clears the Source-Active cache entries for all entries, all sources for a specific group, or all entries for a specific source/group pair.

## MSDP Configuration Examples

This section contains the following MSDP configurations examples:

- Default MSDP Peer
- Logical RP

### Default MSDP Peer

The following example is a partial configuration of Router A and Router C in Figure 63. Each of these ISPs may have more than one customer like the customer in Figure 63 who use default peering (no BGP or MBGP). In that case, they may have similar configurations. That is, they will only accept SAs from a default peer if the SA is permitted by the corresponding prefix list.

#### Router A

```
ip msdp default-peer 10.1.1.1
ip msdp default-peer 10.1.1.1 prefix-list site-a ge 32
ip prefix-list site-b permit 10.0.0.0/8
```

#### Router C

```
ip msdp default-peer 10.1.1.1 prefix-list site-a ge 32
ip prefix-list site-b permit 10.0.0.0/8
```

### Logical RP

The following example configures a logical RP using an MSDP mesh group. The four routers that are logical RPs are RouterA, RouterB, RouterC, and RouterD. RouterE is an MSDP border router that is not an RP. Figure 64 illustrates the logical RP environment in this example; the configurations for routers A, B, and E follow the figure.

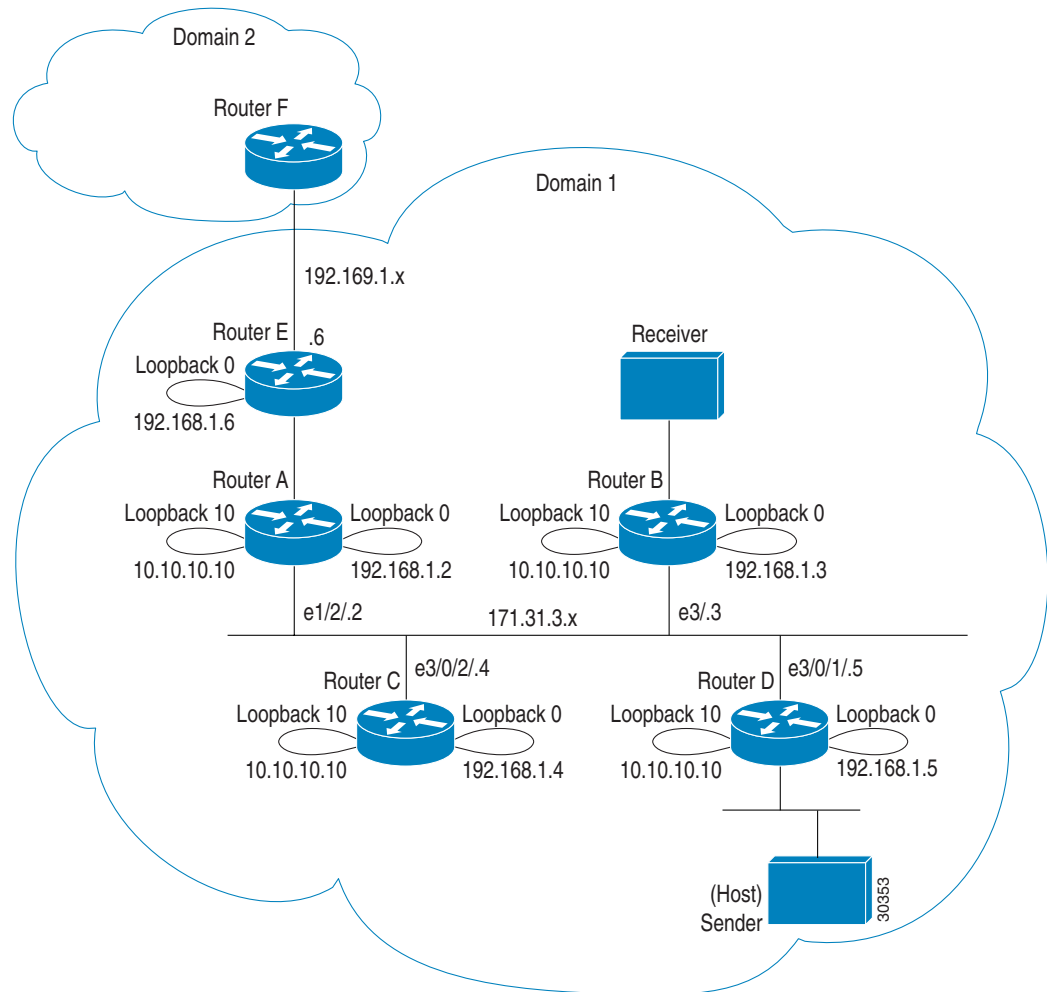
It is important to note the use of the loopback interface and how those host routes are advertised in OSPF. It is also important to carefully choose the OSPF router ID loopback so the ID does not use the logical RP address.

In this example, all the logical RPs are on the same LAN, but this is not typical. The host route for the RP address is advertised throughout the domain and each PIM DR in the domain joins to the closest RP. The RPs share (S, G) information with each other by sending SA messages. Each logical RP must use a separate Originator ID.

Note there are two MSDP mesh groups on RouterA. The routes for the loopback interfaces are in OSPF. Loopback 0 is the Router ID and is used as the connect-source/update-source for MBGP/MSDP. Loopback 10 is the same on all routers in the example.

All networks are 171.69.0.0. The RP address is 10.10.10.10 on Loopback 10 on all RPs. BGP connections are 192.168.1.x on Loopback 0. Loopback 0 is put into BGP with network 192.168.1.3 mask 255.255.255.255 nlri unicast multicast.

**Figure 64 Logical RP Using MSDP**



**RouterA**

```

!
hostname RouterA
!
ip routing
!
ip subnet-zero
ip multicast-routing
!
!
interface Loopback0
 ip address 192.168.1.2 255.255.255.255
 no shutdown
!
interface Loopback10
 ip address 10.10.10.10 255.255.255.255
 no ip directed-broadcast
 ip pim sparse-dense-mode
 no shutdown
!
interface Ethernet1/2
 description LANethernet2
 ip address 171.69.2.2 255.255.255.0
 ip pim sparse-dense-mode
 no shutdown
!
interface Ethernet4/0/0
 description LANethernet3
 ip address 171.69.3.2 255.255.255.0
 ip pim sparse-dense-mode
 no shutdown
!
router ospf 10
 network 171.69.0.0 0.0.255.255 area 0
 network 10.10.10.10 0.0.0.0 area 0
 network 192.168.1.2 0.0.0.0 area 0
!
router bgp 1
 no synchronization
 network 171.69.0.0 nlri unicast multicast
 network 192.168.1.2 mask 255.255.255.255 nlri unicast multicast
 neighbor 192.168.1.3 remote-as 1 nlri unicast multicast
 neighbor description routerB
 neighbor 192.168.1.3 next-hop-self
 neighbor 192.168.1.3 update-source loopback0
 neighbor 192.168.1.4 remote-as 1 nlri unicast multicast
 neighbor description routerC
 neighbor 192.168.1.4 update-source loopback0
 neighbor 192.168.1.5 remote-as 1 nlri unicast multicast
 neighbor description routerD
 neighbor 192.168.1.5 next-hop-self
 neighbor 192.168.1.5 update-source loopback0
 neighbor 192.168.1.6 remote-as 1 nlri unicast multicast
 neighbor description routerE
 neighbor 192.168.1.6 update-source Loopback0
 neighbor 192.168.1.6 next-hop-self
!
!

```

```
ip msdp peer 192.168.1.3 connect-source loopback 0
ip msdp peer 192.168.1.5 connect-source loopback 0
ip msdp peer 192.168.1.4 connect-source loopback 0
ip msdp peer 192.168.1.6 connect-source Loopback0
ip msdp mesh-group inside-test 192.168.1.3
ip msdp mesh-group inside-test 192.168.1.4
ip msdp mesh-group inside-test 192.168.1.5
ip msdp mesh-group outside-test 192.168.1.6
ip msdp cache-sa-state
ip msdp originator-id loopback0
!
ip classless
ip pim send-rp-disc scope 10
ip pim send-rp-anno loopback 10 scope 10
!
```

### RouterB

```
!
hostname RouterB
!
ip routing
!
ip multicast-routing
ip dvmrp route-limit 20000
!
interface Loopback0
 ip address 192.168.1.3 255.255.255.255
 no shutdown
!
interface Loopback10
 ip address 10.10.10.10 255.255.255.255
ip pim sparse-dense-mode
 no shutdown
!
interface Ethernet2
 description LANethernet 0
 ip address 171.69.0.3 255.255.255.0
ip pim sparse-dense-mode
 no shutdown
!
interface Ethernet3
 description LANethernet 2
 ip address 171.69.2.3 255.255.255.0
ip pim sparse-dense
!
router ospf 10
 network 171.69.0.0 0.0.255.255 area 0
 network 10.10.10.10 0.0.0.0 area 0
 network 192.168.1.3 0.0.0.0 area 0
!
router bgp 1
 no synchronization
 network 171.69.0.0 nlri unicast multicast
 network 192.168.1.3 mask 255.255.255.255 nlri unicast multicast
 neighbor 192.168.1.2 remote-as 1 nlri unicast multicast
```

```

neighbor description routerA
neighbor 192.168.1.2 update-source loopback0
neighbor 192.168.1.4 remote-as 1 nlri unicast multicast
neighbor description routerC
neighbor 192.168.1.4 update-source loopback0
neighbor 192.168.1.5 remote-as 1 nlri unicast multicast
neighbor description routerD
neighbor 192.168.1.5 update-source loopback0
neighbor 192.168.1.5 soft-recon in
!
ip msdp peer 192.168.1.2 connect-source loopback 0
ip msdp peer 192.168.1.5 connect-source loopback 0
ip msdp peer 192.168.1.4 connect-source loopback 0
ip msdp mesh-group inside-test 192.168.1.2
ip msdp mesh-group inside-test 192.168.1.4
ip msdp mesh-group inside-test 192.168.1.5
ip msdp cache-sa-state
ip msdp originator-id loopback0
!
ip classless
ip pim send-rp-disc scope 10
ip pim send-rp-anno loopback 10 scope 10
!

```

### RouterE

```

!
hostname RouterE
!
ip routing
!
ip subnet-zero
ip routing
ip multicast-routing
ip dvmrp route-limit 20000
!
interface Loopback0
 ip address 192.168.1.6 255.255.255.255
no shutdown
!
interface Ethernet2
 description LANEthernet 3
 ip address 171.69.3.6 255.255.255.0
 ip pim sparse-dense-mode
no shutdown
!
interface Ethernet5
 description LANEthernet 6
 ip address 192.169.1.6 255.255.255.0
 ip pim sparse-dense-mode
 ip multicast boundary 20
no shutdown
!
router ospf 10
 network 171.69.0.0 0.0.255.255 area 0
 network 192.168.1.6 0.0.0.0 area 0
 default-information originate metric-type 1
!

```

```
router bgp 1
  no synchronization
  network 171.69.0.0 nlri unicast multicast
  network 192.168.1.6 mask 255.255.255.255 nlri unicast multicast
  network 192.168.1.0
  neighbor 192.168.1.2 remote-as 1 nlri unicast multicast
  neighbor 192.168.1.2 update-source Loopback0
  neighbor 192.168.1.2 next-hop-self
  neighbor 192.168.1.2 route-map 2-intern out
  neighbor 192.169.1.7 remote-as 2 nlri unicast multicast
  neighbor 192.169.1.7 route-map 2-extern out
  neighbor 192.169.1.7 default-originate
  !
  ip classless
  ip msdp peer 192.168.1.2 connect-source Loopback0
  ip msdp peer 192.169.1.7
  ip msdp mesh-group outside-test 192.168.1.2
  ip msdp cache-sa-state
  ip msdp originator-id Loopback0
  !
  access-list 1 permit 192.168.1.0
  access-list 1 deny 192.168.1.0 0.0.0.255
  access-list 1 permit any
  !
  route-map 2-extern permit 10
  match ip address 1
  !
  route-map 2-intern deny 10
  match ip address 1
  !
```

