Contents

1 Configuring MSDP

1.1 Introduction

Multicast Source Discovery Protocol (MSDP) is used to connect multiple rendezvous points (RPs) on the multicast network and implement the following two functions.

- Use MSDP among multiple Protocol Independent Multicast Sparse-Mode (PIM-SM) domains to share the multicast source information of these PIM-SM domains to implement cross-domain multicast.

  With the increase of a network, a PIM network can be divided into multiple PIM-SM domains to facilitate management. The RPs in a domain cannot understand multicast source information in other domains. MSDP peers are created among the PIM-SM domains to interact source-active (SA) messages so that multicast source information can be shared and multicast packets can be forwarded to hosts in other domains.

- Use MSDP in a PIM-SM domain to share the multicast source information of multiple RPs to implement an anycast RP.

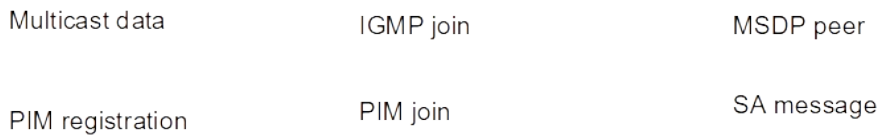
  After RPs in a PIM-SM domain are configured with the same address and MSDP peers are created on these RPs, the RPs can implement load sharing and backup in the PIM-SM domain.

1.1.1 Principles

1. MSDP Peer

Configure one or more pairs of MSDP peers on the network to connect RPs. The peers interact SA messages so that an RP can notify other RPs of the multicast source information on this RP. So far as the unicast route is reachable, the MSDP peer relationship can be established. MSDP peers can be configured on RPs as well as on any other PIM device, for example, X in Figure 1-1.

Figure 1-1 Positions of MSDP Peers



- RP connected to the multicast source

  Configure the MSDP peer on the RP connected to the multicast source. Then, this RP can use SA messages to send the local multicast source information to other RPs.

  As shown in Figure 1-1, DR 1 registers the multicast source information with RP 1. As a peer relationship is established between RP 1 and the PIM device X, RP 1 sends the multicast source information to the PIM device X.

- SA message forwarder

  Non-RPs (common PIM devices) can also act as MSDP peers, but only forward SA messages.

  As shown in Figure 1-1, X forwards SA messages sent from RP 1 to RP 2. In this way, the multicast source information is transferred to RP 2.

- RP connected to the multicast receiver

  Configure the MSDP peer on the RP connected to the multicast receiver. Then, this RP can trigger a join towards the multicast source based on the received SA message.

  As shown in Figure 1-1, DR 2 triggers a join towards RP 2. As RP 2 already obtains the multicast source information, RP 2 continues to trigger a join towards the multicast source, thus establishing a multicast distribution tree (MDT) from DR 1 to DR 2.

2. MSDP Packet

An MSDP packet is encapsulated in a TCP packet and follows the format of type-length-value (TLV), as shown in Figure 1-1.

Figure 1-1 Format of MSDP Packet

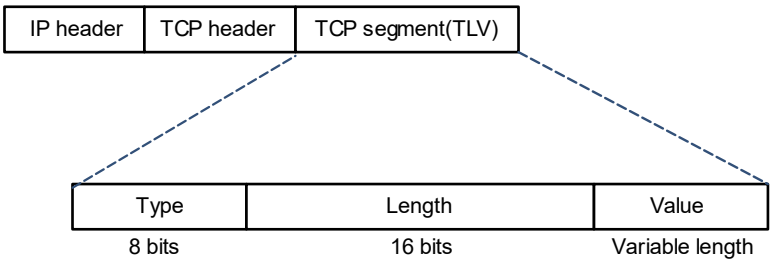


Table 1-1 Fields of MSDP Packet

Field	Length	Description
Type	8 bits	Specifies a message type. ● **1**: Source-Active. Messages of this type carry multiple pairs of (S, G) information and they are transmitted among RPs. PIM-SM multicast packets can be encapsulated in the messages. ● **2**: Source-Active Request. Messages of this type request an (S, G) list of a specified group G to reduce the source join delay. ● **3**: Source-Active Response. Messages of this type are responses to the Source-Active Request. ● **4**: Keep Alive. Messages of this type hold the connection relationship of MSDP peers. ● **5**: Reserved. This is the reserved type of messages. ● **6**: MSDP traceroute in progress. Messages of this type specify the Traceroute function of MSDP and detect the reverse path forwarding (RPF) of SA messages. ● **7**: MSDP traceroute reply. Messages of this type specify the Traceroute function of MSDP and detect the RPF of SA messages.
Length	16 bits	Specifies the length of a message in bytes. The length includes the Type, Length and Value fields. Except for the Keep Alive message, the length of other messages must be 4 bytes at least and 9192 bytes at most.
Value	Subject to the length of the variable	Specifies the message content, which varies with the message type.

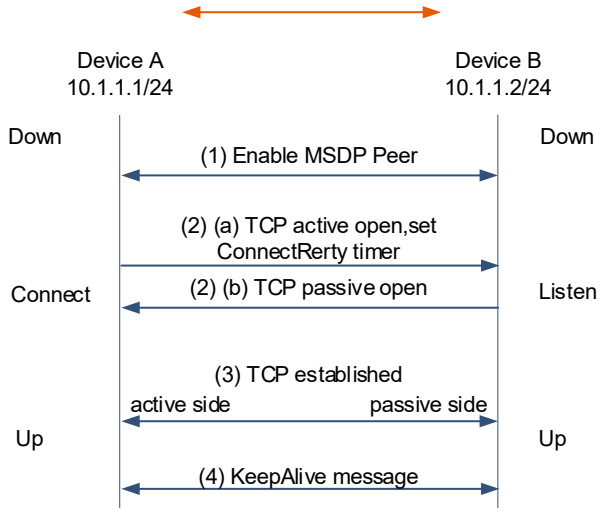
Based on Table 1-1, SA messages can carry multiple pairs of (S, G) information and they are transmitted among RPs. PIM-SM multicast packets can be encapsulated in the messages. The peers interact SA messages with each other to share multicast source information. Multicast packets are encapsulated in the SA messages to avoid the (S, G) entries in the SA messages timeout. If this is the case, hosts cannot receive the multicast packets of the source.

MSDP supports periodic sending of SA requests and SA responses to improve the source information update efficiency. With the mechanism, new hosts do not need to wait for an SA sending period to obtain valid (S, G) information, which reduces the time for the hosts to join a shortest path tree (SPT).

3. MSDP Peer Establishment Procedure

MSDP peers are connected over TCP through port 639. After a TCP connection is established between the peers, the connection is maintained through the keep alive messages.

Figure 1-1 MSDP Peer Connection Establishment Procedure



As shown in Figure 1-1, initially, the MSDP session state of device A and device B is down. The MSDP peer connection establishment procedure is as follows:

(1) Device A and device B specify the other party as a peer mutually and they compare their addresses.

a The IP address of device A is smaller than that of device B. Therefore, device A enters the connection status, initiates a connection request to device B, and starts a timer for reconnection.

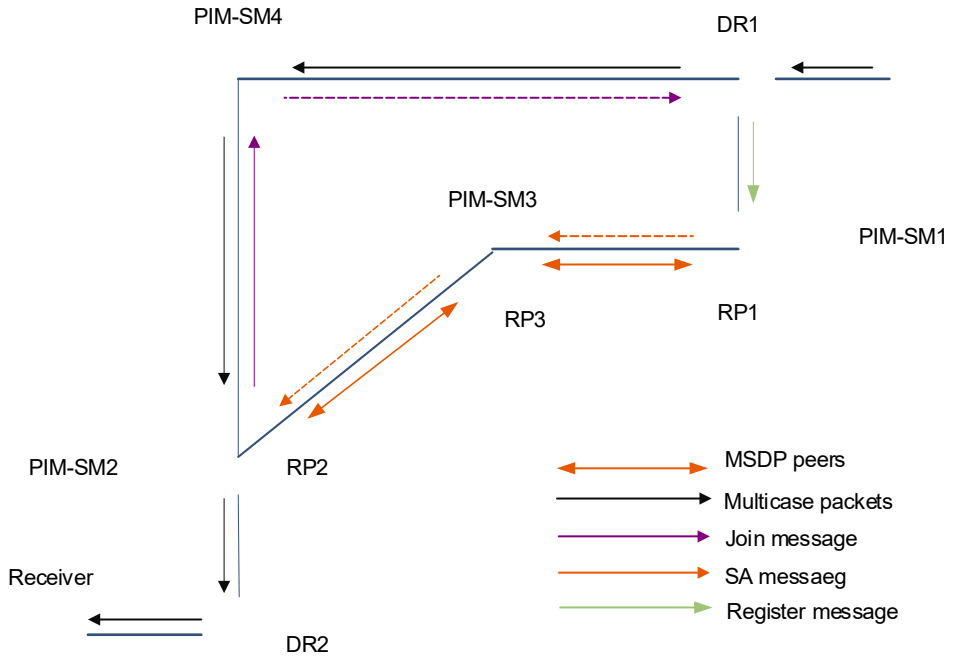
b The IP address of device B is greater. Therefore, device B enters the listening status and waits for the connection request.

(2) After the MSDP session is established between device A and device B, the connection status is up. The two devices send keep alive messages to each other to notify the other party of keeping the MSDP session.

4. Inter-domain Multicast of MSDP

As shown in Figure 1-1, the multicast network is divided into four PIM-SM domains. In PIM-SM 1, the active source sends multicast data to the multicast group and registers with RP 1. In PIM-SM 2, the receiver joins the group, expecting to receive multicast data from the source in PIM-SM 1. The devices in PIM-SM 2 and PIM-SM 3 need to know the position of the source so as to obtain the corresponding multicast data. To implement this purpose, MSDP peer relationship must be established between RP 1 and RP 3 and between RP 3 and RP 2.

Figure 1-1 Inter-domain Multicast of MSDP



The working process of PIM-SM inter-domain multicast is as follows:

(1) The multicast source in PIM-SM 1 sends multicast data to the group. The multicast data is sent to source DR 1 for registration and encapsulated in messages and sent to RP 1. RP 1 obtains the multicast source information.

(2) Source RP 1 sends SA messages to RP 3 periodically. An SA message contains the multicast source address S, multicast group address G, and RP 1 address.

(3) Upon receiving the SA messages, RP 3 performs RPF checking and filters forwarding policies. After the messages pass the checking, they are sent to RP 2. Then, PIM-SM 2 and PIM-SM 3 obtain the source information.

(4) Upon receiving the SA messages, RP 2 checks whether the receiver of the group exists in PIM-SM 2.

- If the receiver exists in PIM-SM 2, an RPT about the group is created between RP 2 and the receiver. RP 2 creates an (S, G) pair and sends an (S, G) join packet to the source hop by hop to generate an SPT. The multicast data is sent to RP 2 along the SPT and then forwarded to the receiver along the RPT. Upon receiving the multicast data, member DR 2 decides whether to perform SPT switchover based on configuration.
- If the receiver does not exist in PIM-SM 2, RP 2 does not create an (S, G) pair or send join packets to the source.

5. Receiving and Forwarding SA Messages

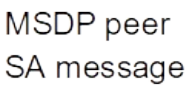
An SA message contains the multicast source address, multicast group address, and RP address. The RP address is the IP address of the RP with which the multicast source is registered.

- The RP encapsulates the locally registered multicast source information in an SA message, and sends the

message to all its MSDP peers.

- On receiving the SA message, each MSDP peer performs the peer RPF check, compares the SA message with the content in the SA cache, and matches the SA message against the SA incoming and outgoing filtering rules. If the SA message passes the peer RPF check and meets the outgoing filtering rules and does not exist in the SA cache, this SA message is forwarded to other MSDP peers.
- For any SA message coming from an MSDP peer (address: N), the following peer RPF check rules are used to prevent loops and avoid SA message flooding:
  a If N is a member of the mesh group, the SA message passes the peer RPF check; otherwise, go to step b.
  b If N is the only active MSDP peer on the local device, the SA message passes the peer RPF check; otherwise, go to step c.
  c If N is the RP address in the SA message, the SA message passes the peer RPF check; otherwise, go to step d.
  d If an EBGP route to the RP address in the SA message exists on the local device and the next hop of this route is N, the SA message passes the peer RPF check; otherwise, go to step e.
  e If an optimum route to the RP address in the SA message exists on the local device, check as follows:
  If this optimum route is a distance vector route (such as the BGP/RIP route), and this router is advertised by N, the SA message passes the peer RPF check.
  If this optimum route is a link status route (such as the OSPF/IS-IS route), and the next hop of this router is N, the SA message passes the peer RPF check.
  Otherwise, go to step f.
  f If an optimum route to the RP address in the SA message exists on the local device, and this route is an MBGP/BGP route, extract the nearest autonomous system (AS) of the AS path of this MBGP/BGP route. If the local device has multiple MSDP peers in this AS and N is the MSDP peer with the largest IP address, or N is the only MSDP peer in this AS, the SA message passes the peer RPF check; otherwise, go to step g.
  g If N is the default MSDP peer, the SA message passes the peer RPF check; otherwise, go to step h.
  h The SA message fails in the peer RPF check.
- When MSDP peer relationship is established on any two members in a group, this group is a mesh group. The mesh group helps reduce the number of SA messages. As shown in Figure 1-2, device B, device C, and device D belong to the same mesh group.
  - For SA messages from device A outside the mesh group and received by device B in the mesh group, after the messages pass the peer RPF check and SA cache comparison, these SA messages are forwarded to other members in the group.
  - For SA messages from device B to device C and device D, they are no longer forwarded to other members in the group.

Figure 1-2 Mesh Group Topology



- The SA cache buffers status of SA messages. Expired SA messages will be deleted.
  - When an MSDP peer receives an SA message

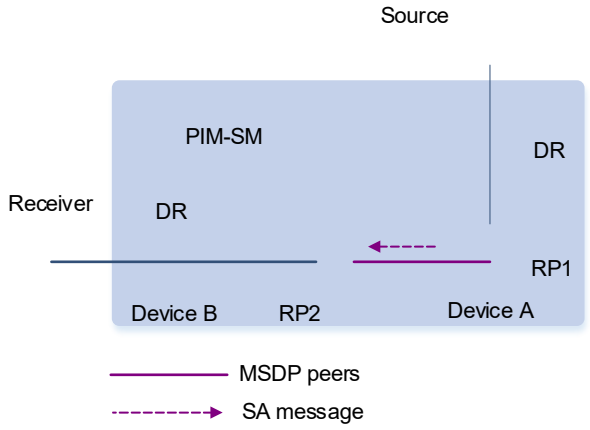
    If this message does not exist in the SA cache and passes the peer RPF check, the message is stored in the SA cache.

    If this message already exists in the SA cache, the message is ignored. This helps suppress SA message flooding.
  - When an MSDP peer receives an SA message, if this message already exists in the SA cache, the message is immediately responded. This helps improve the protocol efficiency.

6. Anycast RP based on MSDP

Generally, each multicast group in a PIM-SM network is served by only one RP. If the RP is faulty or fails, the multicast traffic may be interrupted. Anycast RP enables multiple RPs with the same address to serve a multicast group to implement redundant backup between the RPs. The multicast sources or group members register with the nearest RPs so that the RPs synchronize source information. Anycast RP is implemented by creating MSDP peer relationship between these RPs.

Figure 1-1 Anycast RP based on MSDP



As shown in Figure 1-1, device A and device B in a PIM-SM domain establish peer relationship. The source sends multicast data to the group, and the receiver receives the multicast data as a member of the group. The working process of Anycast RP based on MSDP is as follows:

(1) When the source DR receives the multicast data from the source, the source DR registers with the nearest RP 1.

(2) When the member DR receives a join request packet from the receiver, the member DR forwards the join packet to RP 2. In this way, an RPT with RP 2 as the root is formed.

(3) RP 1 and RP 2 interact SA messages and share the (S, G) information of the multicast source. Upon obtaining the multicast source information, RP 2 sends the join packet to the source hop by hop to generate an SPT.

(4) The multicast data is forwarded to RP 2 through the SPT and then forwarded to the receiver through the RPT. The member DR decides whether to perform SPT switchover based on configuration.

1.1.2 Protocols and Standards

- RFC3618: Multicast Source Discovery Protocol (MSDP)
- RFC 3446: Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)

1.2 Restrictions and Guidelines

Establish the MSDP peer relationship between multiple ASs so that group members can apply for the multicast streams across ASs.

- The inter-AS unicast route must be reachable.
- Run PIM-SM within each AS, and configure the BSR border.
- The IP address and local interface of the MSDP peer must be the same as those of the EBGP peer.

1.3 Configuration Task Summary

The IP multicast configuration includes the following tasks:

(1) Managing MSDP Peers.

- Configuring MSDP Peers
- (Optional) Configuring the Default MSDP Peer
- (Optional) Configuring an MSDP Mesh Group
- (Optional) Configuring the TCP Reconnection Interval of an MSDP Peer
- (Optional) **Enabling MD5 Authentication on TCP Connections Between MSDP Peers**
- (Optional) Configuring the Number of MSDP Peers Supported on a Device

(2) Restricting SA Messages. All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the TTL Value of Multicast Packets in SA Messages
- Enabling the Function of Filtering Source Information Released Locally
- Enabling the Function of Filtering Received SA Requests
- Enabling the Function of Filtering Received SA Messages
-
- Configuring SA Cache Capacity

(3) Configuring an Anycast RP.

1.4 Prerequisites

- Unicast routing protocols are configured and the network in a domain is reachable.
- Basic PIM-SM functions are configured to implement multicast in a domain.

1.5 Managing MSDP Peers

1.5.1 Overview

MSDP peers in different PIM-SM domains interact SA messages to share inter-domain multicast source information.

1.5.2 Configuration Tasks

The MSDP peer management configuration includes the following tasks:

(1) Configuring MSDP Peers

(2) (Optional) Configuring the Default MSDP Peer

(3) (Optional) Configuring an MSDP Mesh Group

(4) (Optional) Configuring the TCP Reconnection Interval of an MSDP Peer

(5) (Optional) Enabling MD5 Authentication on TCP Connections Between MSDP Peers

(6) (Optional) Configuring the Number of MSDP Peers Supported on a Device

1.5.3 Configuring MSDP Peers

1. Overview

MSDP peers are identified based on addresses. The relationship between MSDP peers is bidirectional. Therefore, they must be created on both ends. You can manage MSDP peers by adding description information to a specified MSDP. A connection with a specified peer can be temporarily disabled by configuration.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Establish an MSDP peer relationship.

ip msdp peer *ipv4-peer-address* **connect-source** *interface-type interface-number*

No MSDP peer is added by default.

(4) (Optional) Configure description information for an MSDP peer.

ip msdp description *ipv4-peer-address description*

No description information is added for an MSDP peer by default.

(5) (Optional) Disable an MSDP peer.

ip msdp shutdown *ipv4-peer-address*

The connection with an MSDP peer is enabled by default.

Only the TCP connection with the MSDP peer is disabled, and this MSDP peer and the configuration of this MSDP peer are reserved.

1.5.4 Configuring the Default MSDP Peer

1. Overview

On an MSDP peer, if it is not necessary to perform peer RPF check on SA messages sent from a specified peer, configure this peer as the default peer.

2. Restrictions and Guidelines

- If the **prefix-list** keyword parameter is not specified, all SA messages are accepted.
- If an inexistent **prefix-list** is specified, all SA messages are accepted.
- If an existent **prefix-list** is specified, only the SA messages of RPs specified in this prefix list are accepted.

3. Prerequisites

- An MSDP peer relationship is established.
- If the **prefix-list** keyword parameter is specified, the prefix list must be created before a default MSDP peer is configured. For details about the prefix list configuration, see *Configuring Routing Policies*.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a default MSDP peer.

ip msdp default-peer *ipv4-peer-address* [**prefix-list** *prefix-list-name*]

No default MSDP peer is configured by default.

1.5.5 Configuring an MSDP Mesh Group

1. Overview

When MSDP peer relationship is established on any two members in a group, this group is a mesh group. The mesh group helps reduce the number of SA messages and avoids SA message flooding between the peers. SA messages received by peers in a mesh group are processed in one of the following ways:

- For SA messages coming outside the mesh group, after the SA messages pass the peer RPF check and SA cache comparison, they are forwarded to the other members in the group.
- For SA messages from the internal mesh group, they are received without passing peer RPF check and are no longer forwarded to the other members in the group.

2. Restrictions and Guidelines

Among multiple MSDP peers, if SA messages from these peers pass RPF check by default, these peers can be added to a mesh group.

3. Prerequisites

An MSDP peer relationship is established.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a mesh group.

ip msdp mesh-group *mesh-name ipv4-peer-address*

No mesh group is configured and no MSDP peer is added to any mesh group by default.

1.5.6 Configuring the TCP Reconnection Interval of an MSDP Peer

1. Overview

Within the TCP reconnection interval, the MSDP peer on the proactive connection side can initiate at most one TCP connection. In some application scenarios, for example, MSDP peer creation, restart, or failback, you can shorten the TCP reconnection interval to accelerate convergence of the MSDP peer relationship.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the TCP reconnection interval of an MSDP peer.

ip msdp timer *interval*

The default TCP reconnection interval is **30** seconds.

1.5.7 Enabling MD5 Authentication on TCP Connections Between MSDP Peers

1. Overview

MD5 authentication is enabled on TCP connections between MSDP peers to prevent invalid TCP connections and improve MSDP security. To authenticate the ID of an MSDP peer, you can enable MD5 authentication on the TCP connection established with this MSDP peer.

2. Restrictions and Guidelines

- The MSDP peers must have the consistent configuration, and the ciphers must be the same; otherwise, TCP connections fail.
- If the encryption level is set to 7, the cipher text length must be an even number equal to or greater than 4; otherwise, the configuration fails.
- If the configuration or cipher changes, the local device does not stop the current session. Instead, it attempts to use a new cipher to retain the current session until timeout.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable MD5 authentication on TCP connections between MSDP peers.

ip msdp password peer *ipv4-peer-address* [*encryption-type*] *password-string*

The MD5 authentication function is disabled by default.

1.5.8 Configuring the Number of MSDP Peers Supported on a Device

1. Overview

You can configure the number of MSDP peers supported on a device. If the default number (64) cannot meet requirements, the number of the MSDP peers can be increased.

2. Restrictions and Guidelines

When the number of MSDP peers on the device exceeds the configured number, a notification is displayed to indicate configuration failure. In this case, you need to delete some peers to make the configuration take effect.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the number of MSDP peers supported on a device.

ip msdp peer-limit *peer-limit*

The maximum number of MSDP peers supported on a device is **64** by default.

1.6 Restricting SA Messages

1.6.1 Overview

MSDP peers share multicast source information by exchanging SA messages. Based on the actual network conditions, multicast packets encapsulated in SA messages can be defined, and SA requests and SA messages can be filtered.

1.6.2 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the TTL Value of Multicast Packets in SA Messages
- Enabling the Function of Filtering Source Information Released Locally
- Enabling the Function of Filtering Received SA Requests
- Enabling the Function of Filtering Received SA Messages
-
- Configuring SA Cache Capacity

1.6.3 Prerequisites

MSDP peer relationship is established between devices.

1.6.4 Configuring the TTL Value of Multicast Packets in SA Messages

1. Overview

If the interval of a multicast source for sending multicast data exceeds the timeout of an (S, G) entry, remote users cannot receive the multicast data sent by the multicast source. After the function of encapsulating multicast packets in SA messages is enabled on the source RP, the source RP encapsulates multicast packets in SA messages and sends them to the remote RPs. Upon receiving the messages, the remote RPs decapsulate the messages and transmit the packets in the local domain.

By configuring the time-to-live (TTL) value of multicast packets encapsulated in SA messages, you can control the sending of the multicast packets encapsulated in the SA messages.

- A multicast packet can be sent to MSDP peers only when the TTL value in the IP header of the multicast packet is equal to or greater than the preset TTL value.
- If the TTL value in the IP header of the multicast packet is smaller than the preset TTL value, the multicast packet is removed from the SA message and discarded before the SA message is sent to the MSDP peer.

Therefore, this function affects the sending of multicast packets in SA messages, and does not affect the sending of (S, G) information in the SA messages.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the TTL value of multicast packets in SA messages.

ip msdp ttl-threshold *ipv4-peer-address ttl-value*

The TTL value of the multicast packets in SA messages is not defined by default.

1.6.5 Enabling the Function of Filtering Source Information Released Locally

1. Overview

After source information registered on the local RP is filtered on an MSDP device, only allowed (S, G) information of the local or other domains can be released on the MSDP device.

2. Restrictions and Guidelines

- If the **list** keyword parameter is specified, only the (S, G) information matching this ACL is released.
- If the **route-map** keyword parameter is specified, only the (S, G) information matching this route map is released.
- If these two parameters are specified, only the (S, G) information matching the ACL and route map is released.
- If no parameter is specified, no (S, G) information is released.

3. Prerequisites

Before an IP multicast border is configured, ensure that the corresponding ACL or route map is created and an (S, G) range is specified.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Filter the source information released locally.

ip msdp redistribute [{ **list** *acl-name* | **list** *acl-number* } | **route-map** *route-map-name*] *

All (S, G) information registered on the local RP is released on the MSDP device by default.

1.6.6 Enabling the Function of Filtering Received SA Requests

1. Overview

An MSDP device gives a reply by default when the device receives an SA request. If you want to control the SA request and reply range, you can enable the SA request filtering function on the MSDP device to filter received SA requests.

2. Restrictions and Guidelines

- If the **list** keyword parameter is not specified, all the SA request messages are ignored.
- If the **list** keyword parameter is specified but this ACL is not configured, all SA request messages are ignored.
- If the **list** keyword parameter is specified and this ACL is configured, only the SA requests allowed by the ACL are accepted, and other SA requests are ignored.

3. Prerequisites

Before a received SA request is filtered, ensure that the corresponding ACL is created and a multicast group range is specified.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Filter received SA requests.

ip msdp filter-sa-request *ipv4-peer-address* [{ **list** *acl-name* | **list** *acl-number* }]

All SA request messages from MSDP peers are received and replied by default.

1.6.7 Enabling the Function of Filtering Received SA Messages

1. Overview

By default, SA messages are received and forwarded to other MSDP peers after they pass RPF check. You can configure filtering rules for incoming SA message on the MSDP device to filter received SA messages.

2. Restrictions and Guidelines

- If the function of filtering SA messages is enabled but no ACL or route map is configured, all incoming SA messages are filtered.
- If only one keyword (**list** or **route-map**) is specified and the multicast source (S, G) information in an SA message meets the rule specified by this keyword, this SA message is received.
- If only one keyword (**rp-list** or **rp-route-map**) is specified and the RP address contained in an SA message meets the rule specified by this keyword, this SA message is received.
- If two or more of the keywords (including **list**, **route-map, rp-list** and **rp-route-map**) are specified and the multicast source (S, G) information contained in an SA message meets the rules specified by these keywords, this SA message is received.

3. Prerequisites

Before an IP multicast border is configured, ensure that the corresponding ACL or route map is created and an (S, G) range is specified.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Filter received SA messages.

ip msdp sa-filter in *ipv4-peer-address* [{ **list** *acl-name* | **list** *acl-number* } | **route–map** *route-map-name* | { **rp-list** *acl-name* | **rp-list** *acl-number* } | **rp-route-map** *rp-route-map-name*] *

All SA messages from MSDP peers are received by default.

1.6.8 Enabling the Function of Filtering Sent SA Messages

1. Overview

By default, SA messages are received and forwarded to other MSDP peers after they pass RPF check. You can configure outgoing SA message filtering rules on the MSDP device to filter SA messages to be forwarded.

2. Restrictions and Guidelines

- If the function of filtering sent SA messages is enabled but no ACL or route map is specified, no SA message is sent to other MSDP peers.
- If only one of the keywords (including **list**, **route-map**, **rp-list**, and **rp-route-map**) is specified and the multicast source (S, G) information in an SA message meets the rule specified by this keyword, this SA message is forwarded to other MSDP peers.
- If two or more of the keywords (including **list**, **route-map**, **rp-list**, and **rp-route-map**) are specified and the multicast source (S, G) information in an SA message meets the rules specified by these keywords, this SA message is forwarded to other MSDP peers.

3. Prerequisites

Before an IP multicast border is configured, ensure that the corresponding ACL or route map is created and an (S, G) range is specified.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Filter sent SA messages.

ip msdp sa-filter out *ipv4-peer-address* [{ **list** *acl-name* | **list** *acl-number* } | **route–map** *route-map-name* | { **rp-list** *acl-name* | **rp-list** *acl-number* } | **rp-route-map** *rp-route-map*] *

By default, all SA messages are forwarded to MSDP peers.

1.6.9 Configuring SA Cache Capacity

1. Overview

If an SA cache is used to cache SA messages, the (S, G) entries contained in the SA messages are cached in the SA cache. When a device receives a new join message, the device searches for the SA cache to reduce the delay time of obtaining the multicast information. The more (S, G) entries cached, the greater the used memory space. To suppress SA message flooding, you can limit the number of SA cache entries from a specified MSDP peer or a device.

2. Restrictions and Guidelines

- You are advised to configure the SA cache capacity when you start a device.
- During MSDP running,
  - if the capacity is increased, the adjustment does not affect the SA cache entries that are originally learned.
  - If the capacity is decreased, all SA cache entries learned and initiated must be deleted and re-learned.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Limit the number of SA cache entries from a specified MSDP peer.

ip msdp sa-limit *ipv4-peer-address sa-limit*

The number of SA cache entries from a specified MSDP peer is not limited by default.

(4) (Optional) Configure the SA cache capacity supported on a device.

ip msdp global-sa-limit *sa-limit*

The default SA cache capacity supported on a device is **1024**.

1.7 Configuring an Anycast RP

1.7.1 Overview

RPs in a PIM-SM domain use the same RP address to serve the same group. MSDP peer relationship is established between RPs so that multicast sources and receivers can register with and join the nearest RP. The RPs implement redundancy and load sharing and help accelerate convergence of multicast routes.

1.7.2 Prerequisites

Basic multicast functions are enabled in the PIM-SM domain and multiple RPs are configured for the domain.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Establish an MSDP peer relationship.

ip msdp peer *ipv4-peer-address* **connect-source** *interface-type interface-number*

No MSDP peer is added by default.

(4) Modify the RP address in SA messages.

ip msdp originator-id *interface-type interface-number*

By default, no primary address of an interface is specified as the initiator address in SA messages.

1.8 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

Caution

Running the **clear** commands may lose vital information and thus interrupt services.

Table 1-1 Monitoring

Command	Purpose
clear ip msdp peer *ipv4-peer-address*	Resets the TCP connection with a specified MSDP peer.
clear ip msdp sa-cache [*ipv4-group-address*]	Clears the SA cache.
clear ip msdp statistics [*ipv4-peer-address*]	Clears the statistics of MSDP peers.
show ip msdp count [*as-number*]	Displays the number of sources and the number of groups generated by SA messages.
show ip msdp mesh-group	Displays information of a mesh group.
show ip msdp peer [*ipv4-peer-address*]	Displays detailed information about MSDP peers.
show ip msdp rpf-peer *ipv4-address*	Displays information about the MSDP RPF peer corresponding to the address of a specified initiator.
show ip msdp sa-cache [*ipv4-group-address* | *ipv4-source-address*] [*ipv4-group-address* | *ipv4-*	Displays learned (S, G) information.

Command	Purpose
source-address] [*as-number*]	
show ip msdp sa-originated	Displays (S, G) information initiated by the local device.
show ip msdp summary	Displays summary information of all MSDP peers.
debug ip msdp peer	Debugs MSDP peers.

1.9 Configuration Examples

1.9.1 Enabling Basic Functions of MSDP

1. Requirements

MSDP peers are configured in different domains to connect the RPs. Multicast source information can be shared to other RPs.

2. Topology

Figure 1-1 Topology for Basic Functions of MSDP

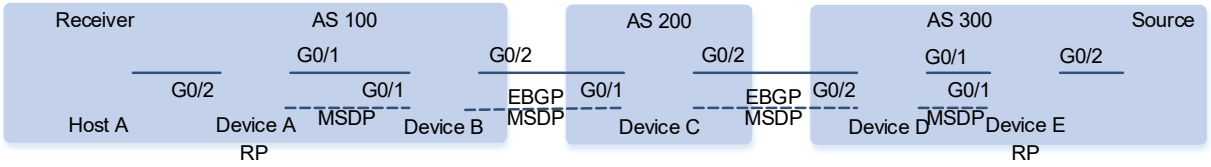


Table 1-1 Description of the Topology

Device	Interface	IP Address	Remarks
Device A	G0/1	10.110.1.1/24	-
	Loopback0	10.10.10.10/32	RP address, which is used to establish an MSDP connection.
Device B	G0/1	10.110.1.2/24	-
	G0/2	10.110.2.1/24	BSR border
	Loopback0	20.20.20.20/32	Used to establish the EBGP and MSDP connections.
Device C	G0/1	10.110.2.2/24	BSR border
	G0/2	10.110.3.1/24	BSR border
	Loopback0	30.30.30.30/32	Used to establish the EBGP and MSDP connections.
Device D	G0/2	10.110.3.2/24	BSR border
	G0/1	10.110.4.1/24	-

Device	Interface	IP Address	Remarks
	Loopback0	40.40.40.40/32	Used to establish the EBGP and MSDP connections.
Device E	G0/1	10.110.4.2/24	-
	Loopback0	50.50.50.50/32	RP address, which is used to establish an MSDP connection.

3. Notes

- Configure an IP address for an interface.
- Enable OSPF in each AS. Establish EBGP peer relationship between AS 200 and AS 100 and between AS 200 and AS 300, and introduce learned BGP and OSPF routes.
- Enable PIM-SM in each AS, configure C-BSRs and C-RPs, and configure the BSR border.
- Establish the MSDP peer relationship between EBGP peers and between the RP and EBGP peers.

⚠ Caution

The IP address and local interface of the MSDP peer must be the same as those of the EBGP peer.

4. Procedure

(1) Configure an IP address for each interface (omitted).

(2) Enable OSPF in each AS. Establish EBGP peer relationship between AS 200 and AS 100 and between AS 200 and AS 300, and introduce BGP and OSPF (omitted). For the omitted information, see *Configuring OSPFv2* and *Configuring BGP*

(3) Enable PIM-SM in each AS, configure C-BSRs and C-RPs, and configure the BSR border.

Configure device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# ip multicast-routing
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface loopback 0
Device A(config-if-Loopback 0)# ip pim sparse-mode
Device A(config-if-Loopback 0)# exit
Device A(config)# ip pim rp-candidate loopback 0
Device A(config)# ip pim bsr-candidate loopback 0
```

Configure device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# ip multicast-routing
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
```

```
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface GigabitEthernet 0/2
Device B(config-if-GigabitEthernet 0/2)# ip pim sparse-mode
Device B(config-if-GigabitEthernet 0/2)# ip pim bsr-border
Device B(config-if-GigabitEthernet 0/2)# exit
Device B(config)# interface loopback 0
Device B(config-if-Loopback 0)# ip pim sparse-mode
Device B(config-if-Loopback 0)# exit
```

Configure device C.

```
Device C>enable
Device C# configure terminal
Device C(config)# ip multicast-routing
Device C(config)# interface GigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device C(config-if-GigabitEthernet 0/1)# ip pim bsr-border
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# interface GigabitEthernet 0/2
Device C(config-if-GigabitEthernet 0/2)# ip pim sparse-mode
Device C(config-if-GigabitEthernet 0/2)# ip pim bsr-border
Device C(config-if-GigabitEthernet 0/2)# exit
Device C(config)# interface loopback 0
Device C(config-if-loopback 0)# ip pim sparse-mode
Device C(config-if-loopback 0)# exit
```

Configure device D.

```
Device D> enable
Device D# configure terminal
Device D(config)# ip multicast-routing
Device D(config)# ip pim ssm default
Device D(config)# interface GigabitEthernet 0/1
Device D(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device D(config-if-GigabitEthernet 0/1)# exit
Device D(config)# interface GigabitEthernet 0/2
Device D(config-if-GigabitEthernet 0/2)# ip pim sparse-mode
Device D(config-if-GigabitEthernet 0/2)# ip pim bsr-border
Device D(config-if-GigabitEthernet 0/2)# exit
Device D(config)# interface loopback 0
Device D(config-if-Loopback 0)# ip pim sparse-mode
Device D(config-if-Loopback 0)# exit
```

Configure device E.

```
Device E> enable
Device E# configure terminal
Device E(config)# ip multicast-routing
Device E(config)# interface GigabitEthernet 0/1
Device E(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device E(config-if-GigabitEthernet 0/1)# exit
```

```
Device E(config)# interface loopback 0
Device E(config-if-Loopback 0)# ip pim sparse-mode
Device E(config-if-Loopback 0)# exit
Device E(config)# ip pim rp-candidate loopback 0
Device E(config)# ip pim bsr-candidate loopback 0
```

(4) Establish the MSDP peer relationship between EBGP peers and between the RP and EBGP peers.

Configure device A.

```
Device A(config)# ip msdp peer 10.10.10.10 connect-source loopback 0
```

Configure device B.

```
Device B(config)# ip msdp peer 10.10.10.10 connect-source loopback 0
Device B(config)# ip msdp peer 30.30.30.30 connect-source loopback 0
```

Configure device C.

```
Device C(config)# ip msdp peer 20.20.20.20 connect-source loopback 0
Device C(config)# ip msdp peer 40.40.40.40 connect-source loopback 0
```

Configure device D.

```
Device D(config)# ip msdp peer 30.30.30.30 connect-source loopback 0
Device D(config)# ip msdp peer 50.50.50.50 connect-source loopback 0
```

Configure device E.

```
Device E(config)# ip msdp peer 50.50.50.50 connect-source loopback 0
```

5. Verification

(1) Use the multicast source to send a packet (200.200.200.200, 225.1.1.1). After a host joins the group 225.1.1.1, this host can receive this packet.

(2) Display the status and SA message of the MSDP peer on device D.

```
Device D# show ip msdp summary
Msdp Peer Status Summary
Peer Address    As    State    Uptime/Downtime    Reset-Count    SA-Count    Peer-
Description
30.30.30.30     200   Up       00:01:420                         1           No
description

Device D# show ip msdp sa-cache
MSDP Source-Active Cache: 1 entries
  (200.200.200.200,225.1.1.1),RP:10.10.10.10,(M)BGP/AS 100, 00:00:18/00:01:57,
Peer 30.30.30.30
Learned from peer 30.30.30.30, RPF peer 30.30.30.30,
SAs received: 1, Encapsulated data received: 1
```

6. Configuration Files

- Device A configuration file

```
!
ip multicast-routing
!
```

```
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface Loopback 0
 ip pim sparse-mode
!
ip msdp peer 10.10.10.10 connect-source Loopback 0
!
ip pim bsr-candidate Loopback 0
ip pim rp-candidate Loopback 0
!
```

- Device B configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface GigabitEthernet 0/2
 no switchport
 ip pim sparse-mode
 ip pim bsr-border
!
interface Loopback 0
 ip pim sparse-mode
!
ip msdp peer 10.10.10.10 connect-source Loopback 0
ip msdp peer 30.30.30.30 connect-source Loopback 0
!
```

- Device C configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
 ip pim bsr-border
!
interface GigabitEthernet 0/2
 no switchport
 ip pim sparse-mode
 ip pim bsr-border
!
```

```
interface Loopback 0
 ip pim sparse-mode
!
ip msdp peer 20.20.20.20 connect-source Loopback 0
ip msdp peer 40.40.40.40 connect-source Loopback 0
!
```

- Device D configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface GigabitEthernet 0/2
 no switchport
 ip pim sparse-mode
 ip pim bsr-border
!
interface Loopback 0
 ip pim sparse-mode
!
ip pim ssm default
!
ip msdp peer 30.30.30.30 connect-source Loopback 0
ip msdp peer 50.50.50.50 connect-source Loopback 0
!
```

- Device E configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface Loopback 0
 ip pim sparse-mode
!
ip msdp peer 50.50.50.50 connect-source Loopback 0
!
ip pim bsr-candidate Loopback 0
ip pim rp-candidate Loopback 0
!
```

7. Common Errors

- The BSR border is not configured, or is not configured on a correct interface.

- PIM-SM is not enabled on the local interface and the peer interface on which MSDP peer connection is established.
- SA messages fail the peer RPF check.

1.9.2 Configuring an Anycast RP

1. Requirements

There are multiple RPs in a PIM domain. After an anycast RP based on MSDP peers is configured, receivers can join the nearest RP, and the multicast source can register with the nearest RP to implement load sharing between the RPs.

2. Topology

Figure 1-1 Anycast RP Topology

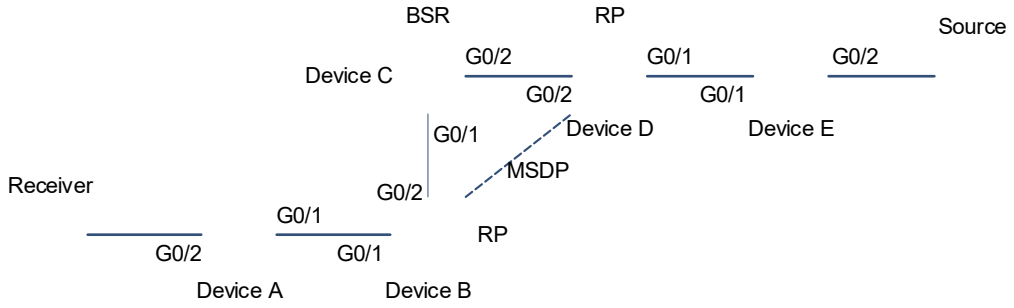


Table 1-1 Description of the Topology

Device	Interface	IP Address	Remarks
Device A	G0/1	10.110.1.1/24	
	G0/2	10.110.2.1/24	
Device B	G0/1	10.110.1.2/24	
	G0/2	10.110.3.1/24	
	Loopback 0	10.10.10.10/32	A C-RP is configured.
	Loopback 1	30.30.30.30/32	Used to establish an MSDP connection and modify the RP address in the SA message.
Device C	G0/1	10.110.3.2/24	
	G0/2	10.110.4.1/24	
	Loopback 0	100.100.100.100/32	A C-BSR is configured.
Device	G0/1	10.110.5.1/24	

Device	Interface	IP Address	Remarks
D	G0/2	10.110.4.2/24	
	Loopback 0	10.10.10.10/32	A C-RP is configured.
	Loopback 1	20.20.20.20/32	Used to establish an MSDP connection and modify the RP address in the SA message.
Device E	G0/1	10.110.5.2/24	
	G0/2	10.110.6.1/24	

3. Notes

- Configure an IP address for each interface.
- Enable OSPF in each AS.
- Enable PIM-SM in each AS, and configure C-BSRs and C-RPs.
- Establish the MSDP peer relationship between RPs, and modify the RP address in the SA message.
- Configure a mesh group.

4. Procedure

(1) Configure an IP address for each interface (omitted).

(2) Enable OSPF in each AS (omitted). For the omitted information, see *Configuring OSPFv2*.

(3) Enable PIM-SM in each AS, and configure C-BSRs and C-RPs.

Configure device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# ip multicast-routing
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface GigabitEthernet 0/2
Device A(config-if-GigabitEthernet 0/2)# ip pim sparse-mode
Device A(config-if-GigabitEthernet 0/2)# exit
```

Configure device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# ip multicast-routing
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface GigabitEthernet 0/2
Device B(config-if-GigabitEthernet 0/2)# ip pim sparse-mode
```

```
Device B(config-if-GigabitEthernet 0/2)# exit
Device B(config)# interface loopback 0
Device B(config-if-Loopback 0)# ip pim sparse-mode
Device B(config-if-Loopback 0)# exit
Device B(config)# interface loopback 1
Device B(config-if-Loopback 1)# ip pim sparse-mode
Device B(config-if-Loopback 1)# exit
Device B(config)# ip pim rp-candidate loopback 0
```

Configure device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# ip multicast-routing
Device C(config)# interface GigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# interface GigabitEthernet 0/2
Device C(config-if-GigabitEthernet 0/2)# ip pim sparse-mode
Device C(config-if-GigabitEthernet 0/2)# exit
Device C(config)# interface loopback 0
Device C(config-if-Loopback 0)# ip pim sparse-mode
Device C(config-if-Loopback 0)# exit
Device C(config)# ip pim bsr-candidate loopback0
```

Configure device D.

```
Device D> enable
Device D# configure terminal
Device D(config)# ip multicast-routing
Device D(config)# interface GigabitEthernet 0/1
Device D(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device D(config-if-GigabitEthernet 0/1)# exit
Device D(config)# interface GigabitEthernet 0/2
Device D(config-if-GigabitEthernet 0/2)# ip pim sparse-mode
Device D(config-if-GigabitEthernet 0/2)# exit
Device D(config)# interface loopback 0
Device D(config-if-Loopback 0)# ip pim sparse-mode
Device D(config-if-Loopback 0)# exit
Device D(config)# interface loopback 1
Device D(config-if-Loopback 1)# ip pim sparse-mode
Device D(config-if-Loopback 1)# exit
Device D(config)# ip pim rp-candidate loopback 0
```

Configure device E.

```
Device E>enable
Device E#configure terminal
Device E(config)#ip multicast-routing
Device E(config)#interface GigabitEthernet 0/1
Device E(config-if-GigabitEthernet 0/1)#ip pim sparse-mode
```

```
Device E(config-if-GigabitEthernet 0/1)# exit
Device E(config)#interface GigabitEthernet 0/2
Device E(config-if-GigabitEthernet 0/2)#ip pim sparse-mode
Device E(config-if-GigabitEthernet 0/2)# exit
```

(4) Establish the MSDP peer relationship between RPs, and modify the RP address in the SA message.

Configure device D.

```
Device D(config)# ip msdp peer 30.30.30.30 connect-source loopback 1
Device D(config)# ip msdp originator-id loopback 1
```

Configure device B.

```
Device B(config)# ip msdp peer 20.20.20.20 connect-source loopback 1
Device B(config)# ip msdp originator-id loopback 1
```

(5) Configure a mesh group.

Configure device D.

```
Device D(config)# ip msdp mesh-group mesh-name 30.30.30.30
```

Configure device B.

```
Device B(config)# ip msdp mesh-group mesh-name 20.20.20.20
```

5. Verification

(1) Use the multicast source to send a packet (6.6.6.6, 225.1.1.1). After a host joins the group 225.1.1.1, this host can receive this packet.

(2) Display the status and SA message of the MSDP peer on device B.

Run the **show ip msdp summary** command to display status of the peers.

```
Device B# show ip msdp summary
Msdp Peer Status Summary
Peer Address    As         State    Uptime/Downtime    Reset-Count    SA-Count
Peer-Description
20.20.20.20     Unknown    Up       00:01:420                         1          No
description
```

Run the **show ip msdp sa-cache** command to display SA messages of the peers.

```
Device B# show ip msdp sa-cache
MSDP Source-Active Cache: 1 entries
  (6.6.6.6,225.1.1.1),RP:10.10.10.10,(M)BGP/AS unknown, 00:00:18/00:01:57,
Peer 20.20.20.20
```

6. Configuration Files

- Device A configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
```

```
!
interface GigabitEthernet 0/2
 no switchport
 ip pim sparse-mode
!
```

- Device B configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface GigabitEthernet 0/2
 no switchport
 ip pim sparse-mode
!
interface Loopback 0
 ip pim sparse-mode
!
interface Loopback 1
 ip pim sparse-mode
!
ip msdp originator-id Loopback 1
ip msdp peer 20.20.20.20 connect-source Loopback 1
ip msdp mesh-group mesh-name 20.20.20.20
!
ip pim rp-candidate Loopback 0
!
```

- Device C configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface GigabitEthernet 0/2
 no switchport
 ip pim sparse-mode
!
interface Loopback 0
 ip pim sparse-mode
!
ip pim bsr-candidate Loopback 0
```

```
!
```

- Device D configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface GigabitEthernet 0/2
 no switchport
 ip pim sparse-mode
!
interface Loopback 0
 ip pim sparse-mode
!
interface Loopback 1
 ip pim sparse-mode
!
ip msdp originator-id Loopback 1
ip msdp peer 30.30.30.30 connect-source Loopback 1
ip msdp mesh-group mesh-name 30.30.30.30
!
ip pim rp-candidate Loopback 0
!
```

- Device E configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface GigabitEthernet 0/2
 no switchport
 ip pim sparse-mode
!
```

7. Common Errors

- The C-BSRs and C-RPs are configured on the same interface.
- The RP address in the SA message is not modified.
- SA messages cannot pass the peer RPF check.

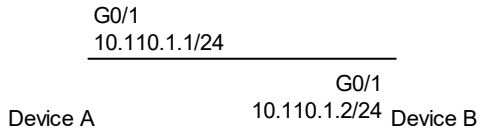
1.9.3 Enabling MD5 Authentication

1. Requirements

MD5 authentication is enabled on TCP connections between MSDP peers, and the number of SA cache entries from a specified MSDP peer is limited to prevent invalid TCP connections and improve MSDP security.

2. Topology

Figure 1-1 Topology of MD5 Authentication



3. Notes

- Establish the MSDP peer relationship between device A and device B.
- Enable MD5 authentication for the peer on device A.
- After MSDP timeout, configure the MD5 cipher of the peer on device B, which is the same as the cipher on device A. Then, the session is reconnected.
- Set the number of SA cache entries from the peer 10.110.1.2 to 10.

4. Procedure

(1) Configure IP addresses on interfaces of device A and device B, and enable basic functions of PIM-SM on the devices (omitted).

(2) Establish the MSDP peer relationship between device A and device B.

Add device B as an MSDP peer on device A.

```
Device A> enable
Device A# configure
Device A(config)# ip msdp peer 10.110.1.2 connect-source gigabitEthernet 0/1
```

Add device A as an MSDP peer on device B.

```
Device B> enable
Device B# configure
Device B(config)# ip msdp peer 10.110.1.1 connect-source gigabitEthernet 0/1
```

(3) Enable MD5 authentication for the peer on device A, and set the encryption level to 0 and the cypher to password123.

```
Device A(config)# ip msdp password peer 10.110.1.2 0 password123
```

(4) After MSDP timeout, enable MD5 authentication for the peer on device B, and set the encryption level and cypher to be consistent with those on device A.

```
Device B(config)# ip msdp password peer 10.110.1.1 0 password123
```

(5) Set the number of SA cache entries from the peer 10.110.1.2 to 10.

```
Device A(config)# ip msdp sa-limit 10.110.1.2 10
```

5. Verification

(1) After the MSDP peer relationship is established between device A and device B, the peer status is up.

Check whether the status of the peer 10.110.1.2 is up on device A.

```
Device A# show ip msdp peer
MSDP PEER 10.110.1.2 (No description), AS unknown
  Connection status:
    State: Up, Resets: 0, Connection source: GigabitEthernet 0/7 (10.110.1.1)
    Uptime(Downtime): 00:01:14, Message sent/received: 2/2
    Input messages discarded: 0
    Connection and counters cleared 00:01:44 ago
    Local Address of connection: 10.110.1.1
  SA Filtering:
    Input (S,G) Access-list filter: None
    Input (S,G) route-map filter: None
    Input RP Access-list filter: None
    Input RP Route-map filter: None
    Output (S,G) Access-list filter: None
    Output (S,G) Route-map filter: None
    Output RP Access-list filter: None
    Output RP Route-map filter: None
  SA-Requests:
    Input filter: None
  Peer ttl threshold: 0
  SAs learned from this peer: 0, SAs limit: No-limit
  Message counters:
    SA messages discarded: 0
    SA messages in/out: 0/0
    SA Requests discarded/in: 0/0
    SA Responses out: 0
    Data Packets in/out: 0/0
```

Check whether the status of the peer 10.110.1.1 is up on device B.

```
Device B# show ip msdp peer
MSDP PEER 10.110.1.1 (No description), AS unknown
  Connection status:
    State: Up, Resets: 0, Connection source: GigabitEthernet 0/1 (10.110.1.2)
    Uptime(Downtime): 00:00:05, Message sent/received: 1/1
    Input messages discarded: 0
    Connection and counters cleared 00:00:14 ago
    Local Address of connection: 10.110.1.2
  SA Filtering:
    Input (S,G) Access-list filter: None
    Input (S,G) route-map filter: None
    Input RP Access-list filter: None
    Input RP Route-map filter: None
    Output (S,G) Access-list filter: None
```

```
    Output (S,G) Route-map filter: None
    Output RP Access-list filter: None
    Output RP Route-map filter: None
  SA-Requests:
    Input filter: None
  Peer ttl threshold: 0
  SAs learned from this peer: 0, SAs limit: No-limit
  Message counters:
    SA messages discarded: 0
    SA messages in/out: 0/0
    SA Requests discarded/in: 0/0
```

(2) After MD5 authentication is enabled for the peer on device A, run the **show ip msdp peer** command to check whether the peer relationship between device A and device B is disconnected and the peer is down.

(3) After MD5 authentication is enabled for the peer on device B, run the **show ip msdp peer** command to check whether the peer relationship between device A and device B is established and the peer is up again.

(4) Set the number of SA cache entries from the peer 10.110.1.2 to 10 on device A, and send 20 (S, G) entries to device B. A message is displayed on device A, indicating that the number of entries exceeds the limit.

6. Configuration Files

- Device A configuration file

```
!
ip msdp peer 10.110.1.2 connect-source gigabitEthernet 0/1
ip msdp password peer 10.110.1.2 0 password123
ip msdp sa-limit 10.110.1.2 10
!
```

- Device B configuration file

```
!
ip msdp peer 10.110.1.1 connect-source gigabitEthernet 0/1
ip msdp password peer 10.110.1.1 0 password123
!
```

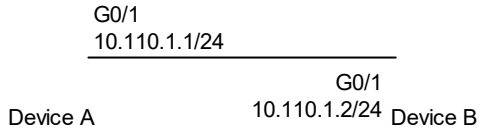
1.9.4 Managing MSDP Peers

1. Requirements

MSDP peer information is managed and configured, including configuring peer description information and disabling peer connections.

2. Topology

Figure 1-1 Topology of MSDP Peer Management



3. Notes

- Establish MSDP peer relationship between device A and device B.
- On device A, configure the peer description of device B as "peer-router-B".
- After 60 seconds, on device A, disable the peer device B.

4. Procedure

(1) Configure IP addresses on interfaces of device A and device B, and enable basic functions of PIM-SM on the devices (omitted).

(2) Establish the MSDP peer relationship between device A and device B.

Add device B as an MSDP peer on device A.

```
Device A> enable
Device A# configure
Device A(config)# ip msdp peer 10.110.1.2 connect-source gigabitEthernet 0/1
```

Add device A as an MSDP peer on device B.

```
Device B> enable
Device B# configure
Device B(config)# ip msdp peer 10.110.1.1 connect-source gigabitEthernet 0/1
```

(3) On device A, configure the peer description of device B as "peer-router-B".

```
Device A(config)# ip msdp description 10.110.1.2 peer-router-B
```

(4) After 60 seconds, on device A, disable the peer device B.

```
Device A(config)# ip msdp shutdown 10.110.1.2
```

5. Verification

Run the **show ip msdp peer** command to display the summary information of a specified peer, including the description and connection status of this MSDP peer.

```
Device A# show ip msdp peer 10.110.1.2
MSDP PEER 10.110.1.2 (peer-router-B), AS unknown
  Connection status:
    State: Up, Resets: 3, Connection source: GigabitEthernet 0/1 (10.110.1.1)
    Uptime(Downtime): 00:30:39, Message sent/received: 50/50
    Input messages discarded: 0
    Connection and counters cleared 00:51:06 ago
    Local Address of connection: 10.110.1.1
  SA Filtering:
    Input (S,G) Access-list filter: None
    Input (S,G) route-map filter: None
    Input RP Access-list filter: None
    Input RP Route-map filter: None
    Output (S,G) Access-list filter: None
    Output (S,G) Route-map filter: None
    Output RP Access-list filter: None
    Output RP Route-map filter: None
```

```
SA-Requests:
  Input filter: None
Peer ttl threshold: 0
SAs learned from this peer: 0, SAs limit: No-limit
Message counters:
  SA messages discarded: 0
  SA messages in/out: 0/0
  SA Requests discarded/in: 0/0
  SA Responses out: 0
  Data Packets in/out: 0/0
```

6. Configuration Files

- Device A configuration file

```
!
ip msdp peer 10.110.1.2 connect-source gigabitEthernet 0/1
ip msdp shutdown 10.110.1.2
ip msdp description 10.110.1.2 peer-router-B
!
```

- Device B configuration file

```
!
ip msdp peer 10.110.1.1 connect-source gigabitEthernet 0/1
!
```

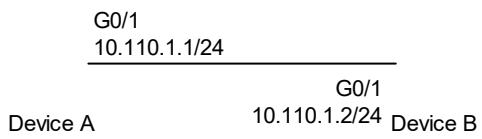
1.9.5 Modifying Protocol Parameters

1. Requirements

In some application scenarios, for example, MSDP peer creation, restart, or failback, you can shorten the TCP reconnection interval to accelerate convergence of the MSDP peer relationship.

2. Topology

Figure 1-1 Topology for Protocol Parameter Modification



3. Notes

- Establish the MSDP peer relationship between device A and device B.
- Set the MSDP peer reconnection interval to 20 seconds on device A.

4. Procedure

(1) Configure IP addresses on interfaces of device A and device B, and enable basic functions of PIM-SM on the devices (omitted).

(2) Establish the MSDP peer relationship between device A and device B.

Add device B as an MSDP peer on device A.

```
Device A> enable
Device A# configure
Device A(config)# ip msdp peer 10.110.1.2 connect-source gigabitEthernet 0/1
```

Add device A as an MSDP peer on device B.

```
Device B> enable
Device B# configure
Device B(config)# ip msdp peer 10.110.1.1 connect-source gigabitEthernet 0/1
```

(3) Set the MSDP peer reconnection interval to 20 seconds on device A.

```
Device(config)# ip msdp timer 20
```

5. Verification

(1) Disable the MSDP peer on device B, and enable the MSDP peer again immediately.

```
Device B(config)# ip msdp shutdown 10.110.1.1
Device B(config)# no ip msdp shutdown 10.110.1.1
```

(2) Check whether the peer on device B can be reconnected in 20 seconds.

```
Device B# show ip msdp peer 10.110.1.1
MSDP PEER 10.110.1.1 (peer-a), AS unknown
  Connection status:
    State: Up, Resets: 3, Connection source: GigabitEthernet 0/1 (10.110.1.2)
    Uptime(Downtime): 00:00:41, Message sent/received: 20/20
    Input messages discarded: 0
    Connection and counters cleared 01:37:02 ago
    Local Address of connection: 10.110.1.2
  SA Filtering:
    Input (S,G) Access-list filter: None
    Input (S,G) route-map filter: None
    Input RP Access-list filter: None
    Input RP Route-map filter: None
    Output (S,G) Access-list filter: None
    Output (S,G) Route-map filter: None
    Output RP Access-list filter: None
    Output RP Route-map filter: None
  SA-Requests:
    Input filter: None
  Peer ttl threshold: 0
  SAs learned from this peer: 0, SAs limit: No-limit
  Message counters:
    SA messages discarded: 0
    SA messages in/out: 0/0
    SA Requests discarded/in: 0/0
    SA Responses out: 0
    Data Packets in/out: 0/0
```

6. Configuration Files

- Device A configuration file

```
!
ip msdp timer 20
ip msdp peer 10.110.1.2 connect-source gigabitEthernet 0/1
!
```

- Device B configuration file

```
!
ip msdp peer 10.110.1.1 connect-source gigabitEthernet 0/1
!
```