



## **MSDP Protocol**

**bintec-Dm 817-I**

Copyright© Version 11.03 bintec elmeg

## Legal Notice

### Warranty

This publication is subject to change.

bintec offers no warranty whatsoever for information contained in this manual.

bintec is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

# Table of Contents

I	Related Documents . . . . .	1
Chapter 1	MSDP Protocol . . . . .	2
1.1	Introduction . . . . .	2
1.1.1	Definitions . . . . .	2
1.1.2	Protocol: Description . . . . .	2
1.1.3	Establishing a connection between MSDP peers . . . . .	3
1.1.4	Types of MSDP messages . . . . .	3
1.1.5	MDSP Peer-RPF Forwarding . . . . .	5
Chapter 2	Configuration . . . . .	9
2.1	Accessing the Configuration menu . . . . .	9
2.2	MSDP Protocol Configuration Commands . . . . .	9
2.2.1	DEFAULT-PEER . . . . .	9
2.2.2	ENABLE . . . . .	10
2.2.3	ORIGINATOR-ID . . . . .	10
2.2.4	PEER . . . . .	11
2.2.5	VRF . . . . .	11
2.2.6	EXIT . . . . .	11
Chapter 3	Monitoring . . . . .	12
3.1	Accessing the Monitoring Menu . . . . .	12
3.2	Monitoring Commands . . . . .	12
3.2.1	LIST . . . . .	12
3.2.2	VRF . . . . .	15
3.2.3	EXIT . . . . .	15
Chapter 4	Examples . . . . .	16
4.1	Example Scenario . . . . .	16
4.1.1	Configuring the devices . . . . .	16



## I Related Documents

bintec-Dm 804-I PIM Protocol

# Chapter 1 MSDP Protocol

## 1.1 Introduction

The Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple PIN-SM domains defined in RFC 3618.

The aim of MSDP is to discover multicast sources in other PIM-SM domains. For further information on the PIM-SM protocol, please see manual bintec-Dm804-I PIM Protocol.

In PIM-SM, the RP is responsible for knowing all the active sources for all the multicast groups in its domain. There can only be one active RP for each given group.

MSDP introduces the ability for the RPs to connect to other RPs and exchange information on the active multicast sources in their respective PIM-SM domains. With this capacity, each domain can connect to another domain.

### 1.1.1 Definitions

#### 1.1.1.1 Roles

##### 1.1.1.1.1 MSDP Peer

The MSDP peers connect using TCP port 639. The lowest IP address takes the active role when executing the TCP connection. The highest IP address waits in a LISTEN state for the other side to establish the connection.

The MSDP peers send *KeepAlive* messages every 60 seconds to maintain the connection active. MSDP messages arriving from peers serve the same function as the *KeepAlive* messages and maintain the session active. If no *KeepAlive* or MSDP messages arrive within 75 seconds, the TCP connection closes.

##### 1.1.1.1.2 Rendezvous Point (RP)

This corresponds to the *Rendezvous Point* role defined in the PIM-SM protocol (bintec-Dm804-I PIM Protocol), but can also have another role within the MSDP protocol. MSDP introduces the ability for RPs to connect to other RPs, to exchange information on the active multicast sources in their respective PIM-SM domains.

##### 1.1.1.1.3 Originating RP

This is the RP that originates the MSDP Source-Active message that the active multicast sources advertise from one PIN-SM domain to other domains.

## 1.1.2 Protocol: Description

The MSDP routers establish peer relationships, similar to BGP peers, on a TCP connection.

Two MSDP peers can be in the same PIM-SM domain or in two different ones.

MSDP enables the RPs to exchange information on multicast sources between different domains, thereby permitting a multicast source discovery between domains to take place.

An RP that wants to participate in the exchange of multicast sources between domains must be an MSDP peer. However, an MSDP peer doesn't have to be an RP. The routers that aren't RPs can be configured as MSDP peers, which is useful in a domain that doesn't support multicast sources but does support the transmission of multicast traffic. An MSDP peer that isn't an RP, doesn't originate information on any multicast source, but does permit the transmission of information on sources from other domains.

When an MSDP peer that is also an RP receives a PIM REGISTER message, it generates an MSDP *Source-Active* (SA) for the peer (*Source, Group*) and sends it to all its configured MSDP peers. The SA message contains the IP address for the multicast source, the IP address for the multicast group and the IP address for the RP.

On receiving an MSDP SA message, the router checks to see whether the message came from its MSDP *RPF-peer*. The rules used to determine the MSDP *RPF-peer* are different from the ones used to determine the *RPF neighbor* in PIM-SM. The rules to determine the MSDP *RPF-peer* will be explained in later chapters in this manual.

If the MSDP SA message has come from an MSDP *peer* that isn't the MSDP *RPF-peer*, the MSDP SA message is ignored and dropped. If the message has come from the MSDP *RPF-peer*, the MSDP SA message is resent to all the MSDP peers. The process of sending MSDP SA messages to all the MSDP peers if the message comes from

the appropriate MSDP peer is known as *peer-RPF flooding*.

If the MSDP peer that received the MSDP SA message is also an RP, an additional process is produced for the MSDP SA message. The RP checks whether there are any members in its domain that are interested in the groups included in the SA message. If there are, the RP resends the multicast traffic over the *shared-tree* for the corresponding multicast group, and sends a PIM JOIN message (S, G) to its *RPF neighbor* to join the *source-tree* (SPT).

MSDP advertises the existence of multicast source. It does not advertise the presence of multicast receivers, which have an advantage, because due to the nature of multicast, there are fewer sources than receivers. Some PIM-SM domains do not have any multicast sources. MSDP provides an additional advantage for these domains that only have receivers, because they can receive traffic without advertising any interest from the multicast group to the rest.

The MSDP routers must maintain a cache with the information received in the MSDP SA messages. The SA message cache is used to reduce flooding; this means that the SA message isn't resent unless it is a new message which has been added to the cache for the first time. This also reduces flooding by advertising the available information every 60 seconds from the cache. Additionally the cache helps diagnose and debug various problems in MSDP. However, this also has a drawback, and that is that it requires a space in the memory that can become very large in order to store all the active multicast sources.

### 1.1.3 Establishing a connection between MSDP peers

MSDP uses the TCP protocol as a transport protocol. This is a peer relationship, where one of the MSDP peers listens to new TCP connections in port 639 (passive MSDP peer) and the other side executes the active connection to this port (active MSDP peer).

The MSDP peer with the highest IP address is the one that listens.

#### 1.1.3.1 MSDP peers state machine

The MSDP peers state machine can take the following states:

##### 1.1.3.1.1 DISABLED

The MSDP peer is not configured. This is the initial state for all the MSDP peers.

##### 1.1.3.1.2 INACTIVE

The MSDP peer is configured but isn't listening or trying to connect.

##### 1.1.3.1.3 CONNECTING

The MSDP peer is an active peer and is trying to initiate the TCP session.

##### 1.1.3.1.4 LISTEN

The MSDP peer is a passive peer and is listening to the connections in TCP port 639.

##### 1.1.3.1.5 ESTABLISHED

The TCP connection has been established.

The normal sequence of states for a **passive** MSDP peer is as follows:

DISABLE # INACTIVE # LISTEN # ESTABLISHED.

The normal sequence of states for an **active** MSDP peer is as follows:

DISABLED # INACTIVE # CONNECTING # ESTABLISHED

The active MSDP peer alternates between the INACTIVE and CONNECTING states until the passive MSDP peer accepts the connection. Each time the active MSDP peer changes from CONNECTING state to INACTIVE, it waits 30 seconds before trying the connection again (*ConnectRetry Timer*).

For further information on the MSDP peers state machine, please see chapter 11 in RFC 3618.

### 1.1.4 Types of MSDP messages

The MSDP protocol sends its messages through the TCP session established between two MSDP peers. Given that the connection is TCP, the messages are always directed to a specific peer.

The MSDP messages take a Type-Length-Value (TLV) format:

Type	Length	Value
8 bits	16 bits	3-9192 octets

The minimum length for an MSDP message is 3 octets and the maximum 9192 octets. Neither the TCP header nor the IP header, nor the layer 2 headers, are included in the 9192 octets.

If a TLV message is received that is longer than the maximum specified (9192 octets), the TLV message should be accepted, but any extra information should be ignored and the MSDP session should not close.

The types of TLV messages defined in RFC 3618 for the MSDP protocol are:

Type	Message
1	IPv4 Source-Active
2	IPv4 Source-Active Request
3	IPv4 Source-Active Response
4	KeepAlive

The messages supported through the implementation available in our routers are detailed below:

### 1.1.4.1 Source-Active

The *Source-Active* (SA) messages are used to advertise sources in a domain. These messages contain the IP address for the *originating RP* and one or more peers (S,G).

The *Source-Active* messages take the following format:

0	31	
Type	Length	Entry Count
RP Address		
Reserved		Sprefix len
Group Address (1)		
Source Address (1)		
...		
Group Address (n)		
Source Address (n)		

- **Type (8 bits):** The SA message corresponds to type 1.
- **Length (16 bits):** this is the sum of two lengths:  $x + y$ 
  - x:** this is the length of the message control information, which corresponds to the two first lines of the message (64 bits), plus 12 times the value that we have filled out in the 'Entry Count' field.
  - y:** This is zero when there is no encapsulated information. In this implementation, information is not encapsulated in the SA message.
- **Entry Count (8 bits):** This is the number of entries that are found after the *RP Address* field.
- **RP Address (32 bits):** This is the RP IP address in the active source domain that has originated the SA message.
- **Reserved (24 bits):** This is a reserved field, which should be transmitted with all zeros, and should be ignored by the receiver.
- **Sprefix Len (8 bits):** This is the length of the route prefix associated with the source IP address. This field should be transmitted with a 32 value (/32).
- **Group Address:** This is the multicast group IP address through which the source sends traffic.
- **Source Address:** This is the active source IP address.

### 1.1.4.2 KeepAlive

A *KeepAlive* message is sent to an MSDP peer if, and only if, MSDP messages have not been sent to the MSDP peer within the 60 seconds considered the KeepAlive period.

This message is necessary to maintain the MSDP connection active.



The *KeepAlive* messages always take the following format:



The length of the message is always 3 octets, which corresponds to the first octet for the type of message and to the two octets for the length of the message.

For further information on the types of MSDP messages, please see chapter 12 in RFC 3618.

## 1.1.5 MDSP Peer-RPF Forwarding

The nature of MSDP is to send MSDP SA messages to all MSDP peers except the peer from which the SA message was received. Because of this behavior, it is possible for an MSDP peer to receive SA messages containing duplicated information from one or more of its peers. However, if the router accepts and sends all these duplicated messages, it would cause unnecessary traffic on the network. To get around this problem, the MSDP protocol uses the *peer-RPF flooding* mechanism to select the peer from which to receive messages.

The RP IP address contained in the SA message is the one used to determine the *RPF peer*. All the SA messages with the same RP IP address have the same *RPF peer*. An SA message is only accepted and forwarded to other peers if it has come from the *RPF peer*, in all other cases it is ignored and silently dropped.

When an SA message is received, the rules are evaluated in order and taking into account all the MSDP peers. The only information used from the SA message is the RP IP address. The source address and the multicast group are not used to determine the *RPF peer*. The MSDP peer that fulfills the first rule will be the *RPF peer*. The SA messages will be accepted and forwarded only when they are received from the *RPF peer*.

### 1.1.5.1 Peer-RPF Route

The *RPF peer* route is a unicast route that is selected for a given IP address. The *RPF peer* route for an RP SA message is used to select the MSDP peer from whom the SA message is accepted.

### 1.1.5.2 Peer-RPF forwarding Rules

Figure 1 represents a basic network diagram that contains relationships between MSDP peers.

The broken lines indicate the relationships existing between MSDP peers.

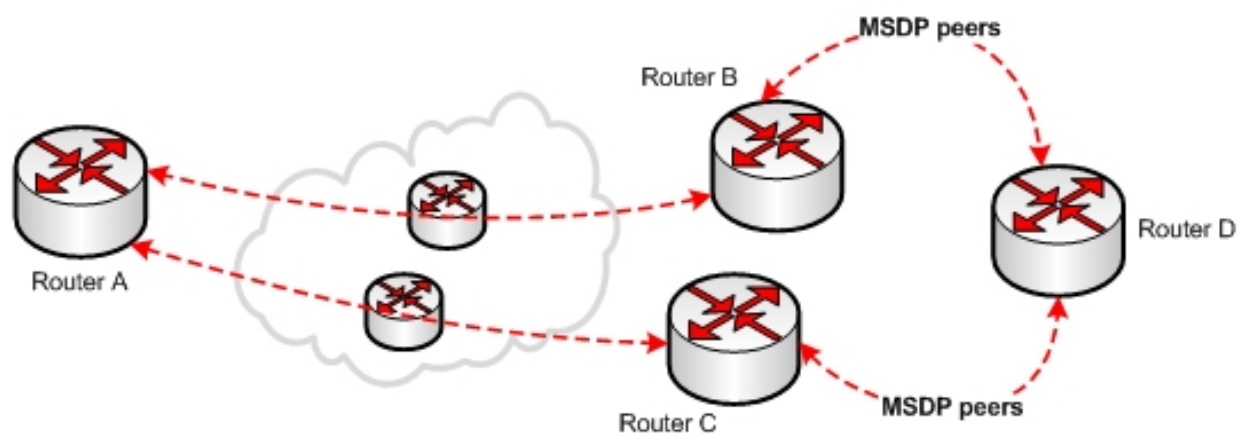


Fig. 1: Network for the RPF peer rules explanation

This figure will be used to describe the rules that permit an *RPF peer* to be determined; this is always from the router D perspective. Router D only has two MSDP peers, which simplifies the explanation of the rules.

#### 1.1.5.2.1 Rule 1



#### Note

“If the originating RP is an MSDP peer, then it is the RPF peer.”

In Figure 1, if router D is an MSDP peer and has an MSDP connection with the *originating RP*, it will use the RP as its *RPF peer*. For example, if router B was the *originating RP*, it will be router D's *RPF peer* for all the SA messages

that router B creates.

For the rest of the rules, we will assume that router A originates the SA messages received by router D.

### 1.1.5.2.2 Rule 2



#### Note

“If the next BGP hop towards the originating RP is an MSDP peer, then this is the RPF peer.”

If any MSDP peer is the next hop in the BGP *peer-RPF* route for the router A address, this MSDP peer will be the *RPF peer*.

In this case, in the Figure 1 diagram, we need to add the BGP relationships that exist between the routers:

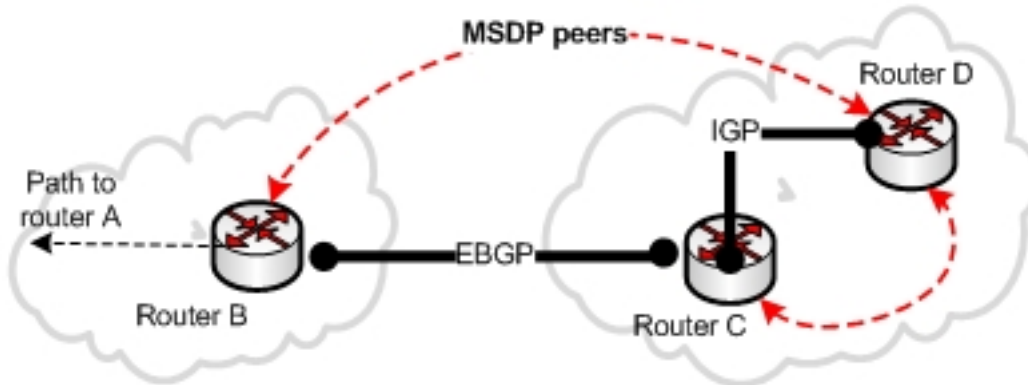


Fig. 2: RPF peer rule 2

If in Figure 2 we assume that the path to reach router A is learnt through router B, then this fulfills rule 2. Router B will be router D's *RPF peer* for the messages received from router A.

### 1.1.5.2.3 Rule 3

The *peer-RPF* route towards the originating RP can be learnt through a distance-vector routing protocol, such as BGP, or through a *link-state* routing protocol, such as OSPF.

For distance-vector routing protocols:



#### Note

“If the *peer-RPF* route to the originating RP is learnt through a distance-vector routing protocol and the MSDP peer is the neighbor that advertises the *peer-RPF* route to the RP, then the MSDP peer is the *RPF peer*.”

For *link-state* routing protocols:



#### Note

“If the *peer-RPF* route to the originating RP is learnt through a *link-state* routing protocol, and the MSDP peer is the next IGP hop to the RP, then the MSDP is the *RPF peer*.”

Here is an example with a *link-state* routing protocol:

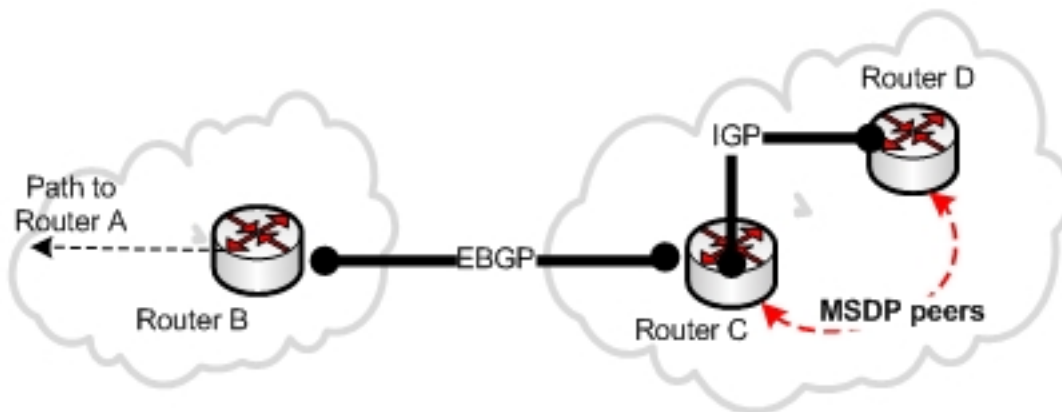


Fig. 3: RPF peer rule 3

In Figure 3 we can see that there is no MSDP peer relationship between router B and router D, so router B can no longer be the *RPF peer* for router D. However, there is an MSDP peer relationship between router C and router D. Additionally, router C is the next IGP hop to the *originating RP* (Router A), consequently it fulfills rule 3 and router C is the *RPF peer*.

#### 1.1.5.2.4 Rule 4



#### Note

“Of all the MSDP peers in the closest Autonomous System (AS) along the path to the originating RP, the MSDP peer with the highest IP address is the RPF peer.”

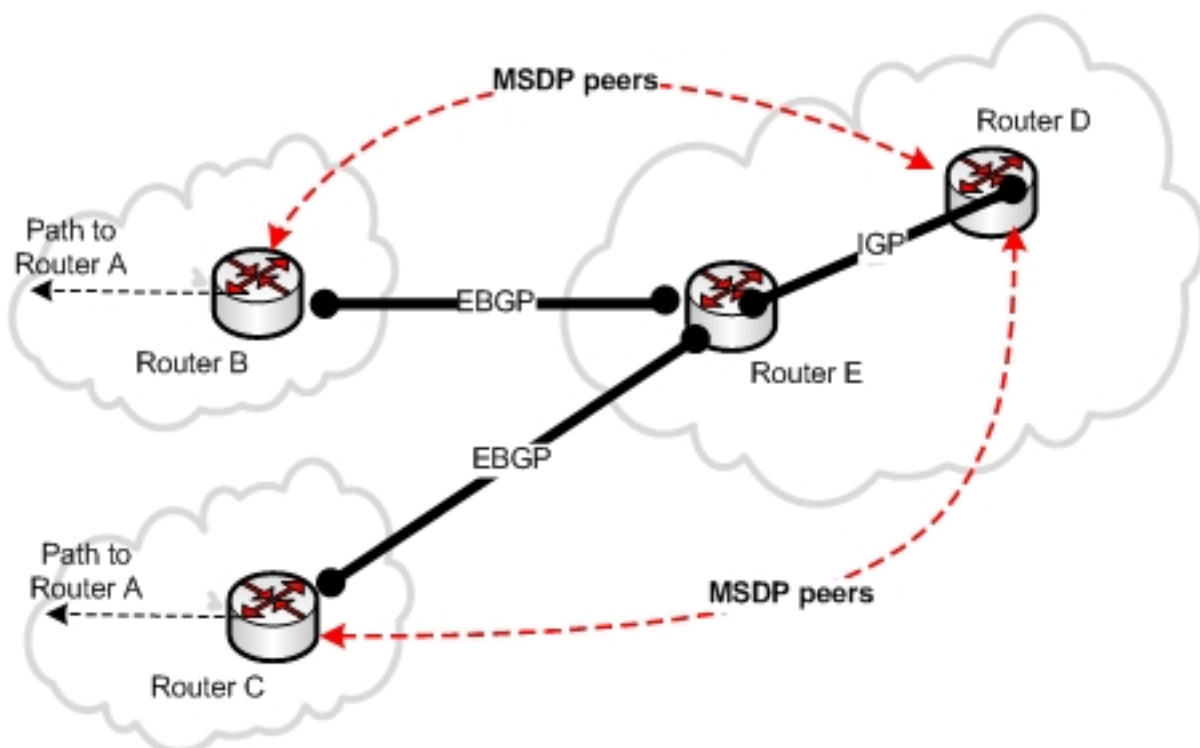


Fig. 4: RPF peer rule 4

In Figure 4, router B and C are MSDP peers for router D. Additionally both routers are in an Autonomous System (AS) along the route to router A.

Let's suppose that the route to router A through router B is shorter, and additionally, router B belongs to the closest AS along the path to the *originating RP* for router D. In this case, router B is the only MSDP peer in the closest AS along the path to router A, and consequently is the *RPF peer*.

In order for router D to know which AS router B belongs to, you need to configure the '*remote-as <as-number>*' option when you configure an MSDP peer.

### 1.1.5.2.5 Rule 5

**Note**

“If you have configured a default MSDP peer for the originating RP, then this is the RPF peer.”

The fifth and last rule is the simplest. The MSDP protocol allows you to configure default MSDP peers. Each default MSDP peer has a range of associated prefixes. This prefix range designates to which originating RPs the default MSDP peer is applicable. If the range of prefixes is 0.0.0.0/0, the default MSDP peer is applied to all the originating RP addresses and is called the *default RPF peer*.

## Chapter 2 Configuration

### 2.1 Accessing the Configuration menu

To access the MSDP protocol configuration menu, you need to enter the following commands at the general prompt:

*Syntax:*

```
*config
Config>protocol msdp
-- MSDP protocol user configuration --
MSDP Config>
```

The MSDP has an independent function through VRF. If you want to configure a VRF that isn't the main one, specify the **vrf** command followed by the name of the VRF.

*Syntax:*

```
MSDP Config>vrf <vrf name>
-- MSDP protocol user configuration for a VRF --
MSDP vrf Config>
```

### 2.2 MSDP Protocol Configuration Commands

The following options appear at the MSDP protocol configuration prompt:

```
MSDP Config>?
  default-peer    Default MSDP peer to accept SA messages from
  enable          Enable MSDP protocol
  no              Negate a command or set its defaults
  originator-id  Configure MSDP Originator ID
  peer            Configure an MSDP peer
  vrf             Specify parameters for a VPN Routing/Forwarding instance
  exit
```

Command	Function
<i>DEFAULT-PEER</i>	Configures a default MSDP peer.
<i>ENABLE</i>	Enables the MSDP in the device.
<i>NO</i>	Allows you to configure the default values or negate a command.
<i>ORIGINATOR-ID</i>	Configures the interface where the IP address used as <i>originating RP</i> in the MSDP SA message is obtained.
<i>PEER</i>	Configures an MSDP peer.
<i>VRF</i>	Configures MSDP in a <i>routing/forwarding</i> domain in private virtual networks (VPN).
<i>EXIT</i>	Exits the MSDP protocol configuration.

#### 2.2.1 DEFAULT-PEER

The **default-peer** command is used to configure a default MSDP peer.

*Syntax:*

```
MSDP Config>default-peer <peer-address> [prefix-list <1..199>]
```

<i>peer-address:</i>	MSDP peer IP address.
<i>prefix-list:</i>	(Optional) Prefix list number (1-199), that allows you to specify the range of <i>originating RPs</i> for which the MSDP peer will be the default MSDP peer.

*Example:*

```
MSDP Config>peer 192.168.1.10
MSDP Config>default-peer 192.168.1.10
MSDP Config>
```

The default MSDP peer must be present as an MSDP peer before being configured as the default peer. If it doesn't exist, the following error message will appear:

```
MSDP Config>default-peer 192.168.2.30
CLI Error: MSDP peer 192.168.2.30 not found
CLI Error: Command error
```

The default MSDP peer allows you to avoid checking whether the received MSDP SA message has been sent by the *RPF peer*, since if the received message is from the default MSDP peer, it's accepted without carrying out any further checks.

If only one MSDP peer has been configured (through the **peer** command), this MSDP peer is used as the default MSDP peer, therefore it's not necessary to configure the default MSDP peer.

If you don't configure the **prefix-list** option, all the MSDP SA messages from the default MSDP peer are accepted.

You can configure multiple default MSDP peers, with or without the prefix-list, in the following way: all the default MSDP peers have prefix lists or none do.

If you configure multiple default MSDP peers with prefix-list, all those default peers are used at the same time for the different RPs.

If you configure multiple MSDP peers without prefix-list, an MSDP peer will be used to accept all the MSDP SA messages. If this MSDP peer drops, then the next configured default MSDP peer is used to accept all the MSDP SA messages.

To delete the **default-peer** command, use the same command preceded by the word "no", specifying which default MSDP peer you wish to delete.

```
MSDP Config>no default-peer 192.168.1.10
```

## 2.2.2 ENABLE

This command allows you to globally enable the MSDP protocol in the device.

*Syntax:*

```
MSDP Config>enable
```

*Example:*

```
MSDP Config>enable
MSDP Config>
```

To disable the MSDP protocol, use the same **enable** command preceded by the word "no":

```
MSDP Config>no enable
```

## 2.2.3 ORIGINATOR-ID

The **originator-id** command enables an MSDP peer that is also an *originating RP* to use the IP address of a specified interface as the RP address for the MSDP SA messages it creates.

*Syntax:*

```
MSDP Config>originator-id <interface>
```

<i>interface:</i>	Name of the interface from which the IP address is derived to be used as the RP address in the MSDP SA message.
-------------------	---

*Example:*

```
MSDP Config>originator-id ethernet0/0
MSDP Config>
```

The selected interface must have an IP address configured or the following error message will be shown:

```
MSDP Config>originator-id ethernet0/1
CLI Error: IP address not configured on that interface
```

```
CLI Error: Command error
```

To delete the MSDP **originator-id** command, use the same command preceded by the word “no”:

```
MSDP Config>no originator-id
```

## 2.2.4 PEER

Use the **peer** command to configure an MSDP peer.

*Syntax:*

```
MSDP Config>peer <peer-address> [connect-source <interface>][remote-as <as-number>]
```

<b>peer-address:</b>	MSDP peer IP address.
<b>interface:</b>	(Optional) Name of the interface from which the IP address is taken as source address for the TCP connection. If you do not configure this option, the IP address of the interface indicating the route to the MSDP peer will be used as source address in the TCP connection.
<b>as-number:</b>	(Optional) Autonomous system number for the MSDP peer. It's important this option is configured when BGP is configured in the router.

*Example:*

```
MSDP Config>peer 192.168.1.10 connect-source ethernet0/0.10 remote-as 100
MSDP Config>peer 192.168.2.30 remote-as 300
```

The interface selected in the **connect-source** option must have an IP address configured or the following error message will appear:

```
MSDP Config>peer 192.168.1.10 connect-source ethernet0/1
CLI Error: IP address not configured on that interface
CLI Error: Command error
MSDP Config>
```

To delete the MSDP peer, use the same command preceded by the word “no”, specifying the MSDP peer you wish to delete:

```
MSDP Config>no peer 192.168.1.10
```

## 2.2.5 VRF

The **vrf** command provides access to the MSDP configuration for the specified VRF. On accessing the MSDP configuration menu for a VRF, the prompt changes to “*MSDP vrf Config>*”. Using the **exit** command will return you to the MSDP configuration for the main VRF.

*Syntax:*

```
MSDP Config>vrf <vrf-name>
```

*Example:*

```
MSDP Config>vrf msdp_vrf
-- MSDP protocol user configuration for a VRF --
MSDP vrf Config>
```

This VRF menu contains the same configuration commands as in the main VRF.

## 2.2.6 EXIT

Use the **exit** command to exit the protocol configuration menu and return to the device configuration prompt.

*Syntax:*

```
MSDP Config>exit
```

*Example:*

```
MSDP Config>exit
Config>
```

## Chapter 3 Monitoring

### 3.1 Accessing the Monitoring Menu

MSDP protocol monitoring shows information relative to the functioning of the protocol.

To access the MSDP protocol monitoring menu, you need to enter the following commands at the general prompt:

*Syntax:*

```
*monitor
Console Operator
+protocol msdp
-- MSDP protocol monitor --
MSDP+
```

The MSDP has an independent function through VRF. If you want to access a VRF that isn't the main one where MSDP is active, specify the **vrf** command followed by the name of the VRF. If the MSDP isn't enabled in the VRF, the VRF MSDP monitoring menu cannot be accessed even though said VRF exists.

*Syntax:*

```
MSDP Config>vrf <vrf name>

-- MSDP protocol user configuration for a VRF --
MSDP vrf Config>
```

### 3.2 Monitoring Commands

The following options appear at the MSDP protocol monitoring prompt:

```
MSDP+?
  list      List MSDP information
  vrf       MSDP monitoring in a VPN Routing/Forwarding instance
  exit
MSDP+
```

Command	Function
<i>LIST</i>	Lists information on the current status of the MSDP protocol.
<i>VRF</i>	Selects another VRF instance where the MSDP protocol function is monitored.
<i>EXIT</i>	Exits the MSDP protocol monitoring.

#### 3.2.1 LIST

The **list** command displays information gathered by the MSDP protocol.

*Syntax:*

```
MSDP+list ?
  peer      MSDP peer status
  sa-cache  MSDP Source-Active cache
```

##### 3.2.1.1 LIST PEER

This command displays information on the MSDP peers.

*Syntax:*

```
MSDP+list peer ?
  <a.b.c.d>  IP address of MSDP peer
  detailed  Show advanced information about MSDP peer
  <cr>
```



### 3.2.1.1.1 LIST PEER

Displays the full list of the MSDP peers without any filters.

**Syntax:**

```
MSDP+list peer
```

**Example:**

```
MSDP+list peer
```

```
MSDP Peer list
```

```
-----
MSDP Peer      State      Resets  Uptime      Connection-source
-----
192.168.1.10   Up         0       51m15s     ethernet0/0.10
192.168.2.30   Up         0       51m5s      none configured
```

The configured MSDP peers are displayed together with the associated information. The following is cited for each peer:

- **MSDP Peer:** MSDP peer IP address.
- **State:** State the MSDP peer is in. The possible states are as follows:
  - **Down:** indicates that there is no active connection with this MSDP peer. This corresponds to the DISABLED state for the MSDP peers state machine.
  - **Inactive:** Indicates that the connection with the MSDP peer is in an inactive state. This corresponds to the same state (inactive) in the MSDP peers state machine.
  - **Connecting:** Indicates that this is trying to connect to the MSDP peer. This corresponds to the same state (connecting) in the MSDP peers state machine.
  - **Listen:** Indicates that this is waiting for a connection from the MSDP peer. This corresponds to the same state (listen) in the MSDP peers state machine.
  - **Up:** Indicates that there is an active connection with this MSDP peer. This corresponds to the ESTABLISHED state for the MSDP peers state machine.
- **Resets:** Indicates the number of times that the connection with this MSDP peer has reset.
- **Uptime:** Time that the MSDP peer has been active.
- **Connection-source:** Interface used to obtain the IP address used as the source address by the TCP connection. If this option is not configured, 'none configured' is displayed.

### 3.2.1.1.2 LIST PEER <PEER-ADDRESS>

Only lists the MSDP peer specified in the '*peer-address*' option.

**Syntax:**

```
MSDP+list peer <peer-address>
```

**Example:**

```
MSDP+list peer 192.168.1.10
```

```
MSDP Peer list
```

```
-----
MSDP Peer      State      Resets  Uptime      Connection-source
-----
192.168.1.10   Up         0       51m22s     ethernet0/0.10
```

### 3.2.1.1.3 LIST PEER DETAILED

Shows detailed information on all the MSDP peers.

**Syntax:**

```
MSDP+list peer detailed
```

**Example:**

```
MSDP+list peer detailed
```

```
MSDP Peer list
```

```
-----
MSDP peer: 192.168.1.10 , AS 100
Connection status:
  State: Up
  Connection source: ethernet0/0.10
  Uptime: 51m42s
  Resets: 0
  Messages stats: Sent: 51 / Received: 52
  SA from this peer: Learned: 4 / Rejected: 0

MSDP peer: 192.168.2.30 , AS 300
Connection status:
  State: Up
  Connection source: none configured
  Uptime: 51m32s
  Resets: 0
  Messages stats: Sent: 47 / Received: 51
  SA from this peer: Learned: 0 / Rejected: 0
```

This displays the configured MSDP peers and their detailed information. For each peer the following is cited:

- **MSDP Peer:** MSDP peer IP address.
- **AS:** Autonomous system number the MSDP peer belongs to. This corresponds to the '*remote-as*' option for the MSDP peers configuration. If you don't specify this option in the configuration, 'none configured' is displayed.
- **Connection status:** The first four lines correspond to information already described in the previous sections, consequently we are only going to detail the new lines:

**Messages stats:** MSDP message statistics.

- **Sent:** Number of MSDP messages sent to the MSDP peer.

- **Received:** Number of MSDP messages received from the MSDP peer.

**SA from this peer:** MSDP SA message statistics.

- **Learned:** Number of active multicast sources learnt through the MSDP SA messages received from this MSDP peer.

- **Rejected:** Number of rejected MSDP SA messages that have been received from this MSDP peer.

### 3.2.1.2 LIST SA-CACHE

Permits you to display the information contained in the MSDP SA messages cache.

**Syntax:**

```
MSDP+list sa-cache
```

**Example:**

```
MSDP+list sa-cache
```

```
Multicast Source Discovery Protocol - Source Active Cache
```

```
-----
Source address  Group address  RP address      Peer address    Uptime/Lifetime
-----
10.0.0.9        239.0.0.3      10.10.10.10     192.168.1.10   8m14s/1m27s
10.0.0.13       239.0.0.4      10.10.10.10     192.168.1.10   8m1s/1m27s
10.0.0.5        239.0.0.2      10.10.10.10     192.168.1.10   8m28s/1m27s
10.0.0.17       239.0.0.5      10.10.10.10     192.168.1.10   7m38s/1m27s
```

```
Number of MSDP SA Cache entries listed: 4
```

The following information is given for each entry:

- **Source address:** Source IP address.
- **Group address:** Multicast group IP address.
- **RP address:** IP address of the RP that has originated the message (*originating RP*).
- **Peer address:** IP address of the MSDP peer that the messages have come from.
- **Uptime:** Time the entry has been installed in the cache.
- **Lifetime:** Remaining lifetime for the entry. If this hasn't received an SA message during this time, the entry is deleted from the cache.

### 3.2.2 VRF

The **vrf** command allows you to access the MSDP protocol monitoring menu for the VRF *vrf\_name*. For this to be possible, said VRF must already exist and have the MSDP protocol enabled. The main VRF of the router is monitored in the main MSDP protocol monitoring menu, and is available even though MSDP is not enabled in it. The **vrf** command is not present in a VRF protocol menu if it is not the router's main vrf.

*Syntax:*

```
MSDP+vrf <vrf-name>
```

*Example:*

```
MSDP+vrf msdp_vrf
-- MSDP protocol monitor for a VRF --
MSDP vrf+
```

This VRF menu contains the same configuration commands as in the main VRF.

### 3.2.3 EXIT

Use the **exit** command to exit the protocol monitoring menu and return to the device monitoring prompt.

*Syntax:*

```
MSDP+exit
```

*Example:*

```
MSDP+exit
+
```

## Chapter 4 Examples

### 4.1 Example Scenario

This example scenario illustrates how to configure different MSDP devices, in a simple scenario, with different roles: RP and MSDP peer.

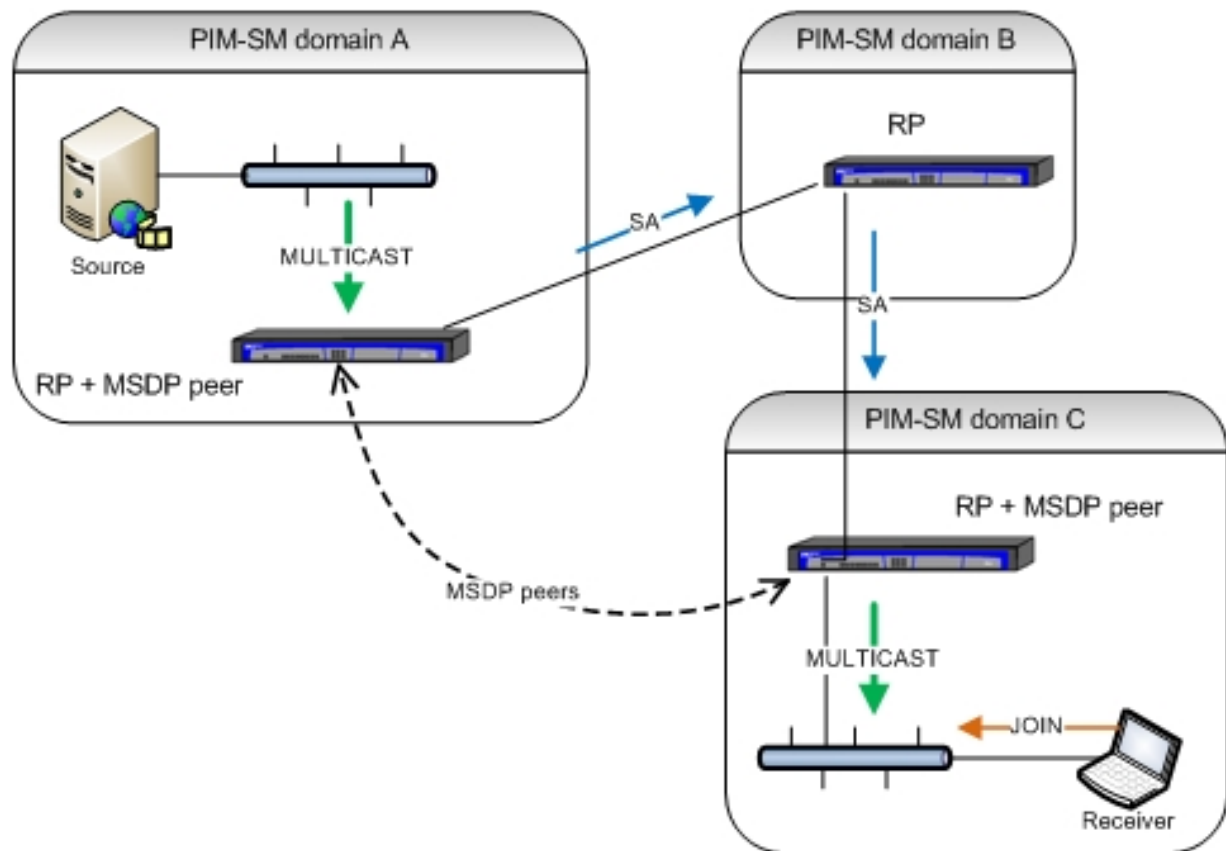


Fig. 5: Example scenario

#### 4.1.1 Configuring the devices

### 4.1.1.1 Configuring the A domain device

```
log-command-errors
no configuration
add device eth-subinterface ethernet0/0 10
add device loopback 10
network ethernet0/0
; -- Ethernet Interface User Configuration --
  description to_SRC
;
  ip address 10.10.0.1 255.0.0.0
;
  ip pim sparse-mode
;
exit
;
network loopback10
; -- Loopback interface configuration --
  description RP
;
  ip address 10.10.10.10 255.255.255.255
;
  ip pim sparse-mode
;
exit
;
network ethernet0/1.10
; -- Ethernet Subinterface Configuration --
  description peering
;
  ip address 192.168.1.10 255.255.255.0
;
  ip pim bsr-border
  ip pim sparse-mode
;
  encapsulation dot1q 10
;
exit
;
protocol msdp
; -- MSDP protocol user configuration --
  enable
  peer 192.168.2.30 connect-source ethernet0/1.10 remote-as 300
;
exit
;
protocol pim
; -- PIM protocol user configuration --
  enable
;
  rp-address 10.10.10.10
;
exit
;
protocol ip
; -- Internet protocol user configuration --
  router-id 10.10.0.1
  exit
;
protocol bgp
; -- Border Gateway Protocol user configuration --
  enable
;
  as 100
  export as 200 prot all all
;
group type external peer-as 200
```

```
; -- BGP group configuration --
    peer 192.168.1.20
    exit
;
exit
;
dump-command-errors
end
```

MSDP has been enabled and the router in domain C (192.168.2.30) has been configured as the MSDP peer.

Additionally, the router itself has been configured as the domain A RP (10.10.10.10) and as *bsr-border* in the *ether-net0/1.10* interface, as this is a border router for domain A in this interface.

BGP is also configured to allow routing information to be exchanged with the domain B router (192.168.1.20).

### 4.1.1.2 Configuring the B domain device

```

log-command-errors
no configuration
add device eth-subinterface ethernet0/0 10
add device loopback 10
network ethernet0/1
; -- Ethernet Interface User Configuration --
  ip address 192.168.2.20 255.255.255.0
;
  ip pim bsr-border
  ip pim sparse-mode
;
exit
;
network loopback10
; -- Loopback interface configuration --
  description RP
;
  ip address 20.20.20.20 255.255.255.255
;
  ip pim sparse-mode
;
exit
;
network ethernet0/0.10
; -- Ethernet Subinterface Configuration --
  ip address 192.168.1.20 255.255.255.0
;
  ip pim bsr-border
  ip pim sparse-mode
;
  encapsulation dot1q 10
;
exit
;
protocol pim
; -- PIM protocol user configuration --
  enable
;
  rp-address 20.20.20.20
;
exit
;
protocol ip
; -- Internet protocol user configuration --
  router-id 192.168.1.20
  exit
;
protocol bgp
; -- Border Gateway Protocol user configuration --
  Enable
;
  as 200
  export as 100 prot all all
;
  export as 300 prot all all
;
  group type external peer-as 100
; -- BGP group configuration --
  peer 192.168.1.10
  exit
;
  group type external peer-as 300
; -- BGP group configuration -
  peer 192.168.2.30

```

```
    exit
;
    Exit
;
    dump-command-errors
end
```

This router is not an MSDP peer; it's only the RP for the B domain (20.20.20.20).

Additionally, the router has also been configured as *'bsr-border'* in the *ethernet0/1* and *ethernet0/0.10* interface, as this is a border router for domain B in these interfaces.

BGP is also configured to allow routing information to be exchanged with both the domain A router (192.168.1.10) and the domain C router (192.168.2.30).



### 4.1.1.3 Configuring the C domain device

```
log-command-errors
no configuration
add device loopback 10
network ethernet0/0
; -- Ethernet Interface User Configuration --
    description peering
;
    ip address 192.168.2.30 255.255.255.0
;
    ip pim bsr-border
    ip pim sparse-mode
;
exit
;
network loopback10
; -- Loopback interface configuration --
    description RP
;
    ip address 30.30.30.30 255.255.255.255
;
    ip pim sparse-mode
;
exit
;
        protocol msdp
        ; -- MSDP protocol user configuration --
            enable
            peer 192.168.1.10 connect-source ethernet0/0 remote-as 100
;
        exit
;
protocol pim
; -- PIM protocol user configuration --
    enable
;
    rp-address 30.30.30.30
;
exit
;
protocol ip
; -- Internet protocol user configuration --
    router-id 192.168.2.30
exit
;
protocol bgp
; -- Border Gateway Protocol user configuration --
    enable
;
    as 300
    export as 200 prot all all
;
    group type external peer-as 200
; -- BGP group configuration --
        peer 192.168.2.20
        exit
;
exit
;

dump-command-errors
end
```

MSDP has been enabled and the router in domain A (192.168.1.10) has been configured as the MSDP peer.

Additionally, the router itself has been configured as the domain C RP (30.30.30.30) and as '*bsr-border*' in the *ether-net0/0* interface, as this is a border router for domain C in this interface.

BGP is also configured to allow routing information to be exchanged with the domain B router (192.168.2.20).