

Multicast VPN

Overview

A separate function is required to enable IP multicast over a Multiprotocol Label Switching Virtual Private Networks (MPLS VPNs) network, as MPLS has no native ability to support it. This document will enable network administrators to configure Multicast VPNs (MVPNs) on an existing MPLS VPN.

This design guides assumes that the reader has previous knowledge about IP multicast and MPLS. For readers unfamiliar with these topics, please visit:

- MPLS VPNs

http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a00800a6c11.shtml

- IP Multicast

<http://www.cisco.com/go/ipmulticast>

- MVPNs Command Reference

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00801039b0.html

- MVPNs White Paper:

http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a00800a3db6.shtml

At the conclusion of this document, the reader should understand the concepts of MVPN, as well as the PIM options available to the Service Provider core and

the customer network. The reader should also be able to configure and troubleshoot a MVPN deployment.

Terminology

- *CE*: Customer Edge Router

Router at the edge of the customer network that has interfaces to at least one PE router

- *Data-MDT*

Tree created dynamically by the existence of active sources in the customer network sending to active receivers located behind separate PE routers. Data MDT will only connect to PE routers that are either attached to CE routers with active sources or receivers of traffic from active sources or that are directly attached to active sources or receivers of traffic.

- *Default-MDT*

Tree created by the MVPN configuration. The Default-MDT is used for customer Control Plane and low rate Data Plane traffic. It connects all of the PE routers with MVRFs in a particular MD and one will exist in every MD whether there is any active source in the respective customer network.

- *LEAF*

Describes the recipient of multicast data, the source is thought of as the route and the destination the leaf



- *MD*: Multicast Domain
Collection of MVRFs that can exchange multicast traffic
- *MDT*: Multicast Distribution Tree
- *MVRF*: Multicast VRF *MVPN*: Multicast VPNP: Provider Router
Router in the core of the provider network that only has interfaces to other P routers and other PE routers
- *PE*: Provider Edge Router
Router at the edge of the provider network that has interfaces to other P and PE routers and to at least one CE router
- *PIM*: Protocol Independent Multicast
- *PIM-Bi-Dir*: Bi-directional
- *PIM-DM*: Dense Mode
- *PIM-SM*: Sparse Mode
- *PIM-SSM*: Source Specific Mode
- *RP*: Rendezvous Point
- *RPF*: Reverse Path Forwarding
- *VPN*: Virtual Private Network
- *VRF*: VPN Routing and Forwarding

Basic Concept of MVPN

The basic concept of MVPN is as follows:

- The Service Provider has an IP Network with its own unique IP multicast domain (ie: P-Network).
- The MVPN customer has an IP Network with its own unique IP multicast domain (ie: C-Network).
- The Service Provider MVPN network forwards the customer IP multicast data to remote customer sites. To achieve this, customer traffic (C-packets) is encapsulated at the Service Provider PE inside P-packets. The encapsulated P-packet is then forwarded to remote PE sites as native multicast inside the P-Network
- During this process, the P-Network has no knowledge of the C-Network traffic. The PE is the device that participates in both networks. Note there may be more than one Customer Network per PE.

Multicast Routing Inside the VPN Versus Multicast Routing Inside the Provider Network

A PE router an MVPN network has multiple multicast routing tables, as well as multiple instances of PIM, IGMP, and MSDP. There is one global table and a table per MVRF.

Multicast Domains is based on the principle of encapsulating multicast packets from a VPN in multicast packets to be routed in the core. As multicast is used in the core network, PIM must be configured in the core.

PIM-SM, PIM-SSM, and PIM-BIDIR are all supported inside the provider core for MVPN.

PIM-SM or PIM-SSM is the recommended PIM option in the provider core, because PIM-BIDIR is not yet supported by all platforms, PIM-SM, PIM-SSM, PIM-BIDIR and PIM-DENSE-MODE are supported inside the MVPN.



MVPN has the concepts of Multicast Distribution Trees (MDT). An MDT is sourced by a PE router and has a multicast destination address. PE routers that have sites for the same MVPN will all source to a Default-MDT and also join to receive traffic on it.

There is a distinction between Default-MDTs and Data-MDTs. A Default-MDT is a tree that is 'always-on' and will transport PIM control-traffic, dense-mode traffic and rp-tree (*,G) traffic. All PE routers configured with the same default-MDT will receive this traffic.

Data-MDTs are trees that are created on demand and will only be joined by the PE routers that have interested receivers for the traffic. They can be created either by a traffic rate threshold and/or source-group pair.

Default-MDTs must have the same group address for all VRFs that comprise a MVPN. Data-MDTs may have the same group address if PIM-SSM is used. If PIM-SM is used, they must have a different group address, as providing the same one could result in the PE router receiving unwanted traffic. This is a PIM-SM protocol issue, not an implementation issue.

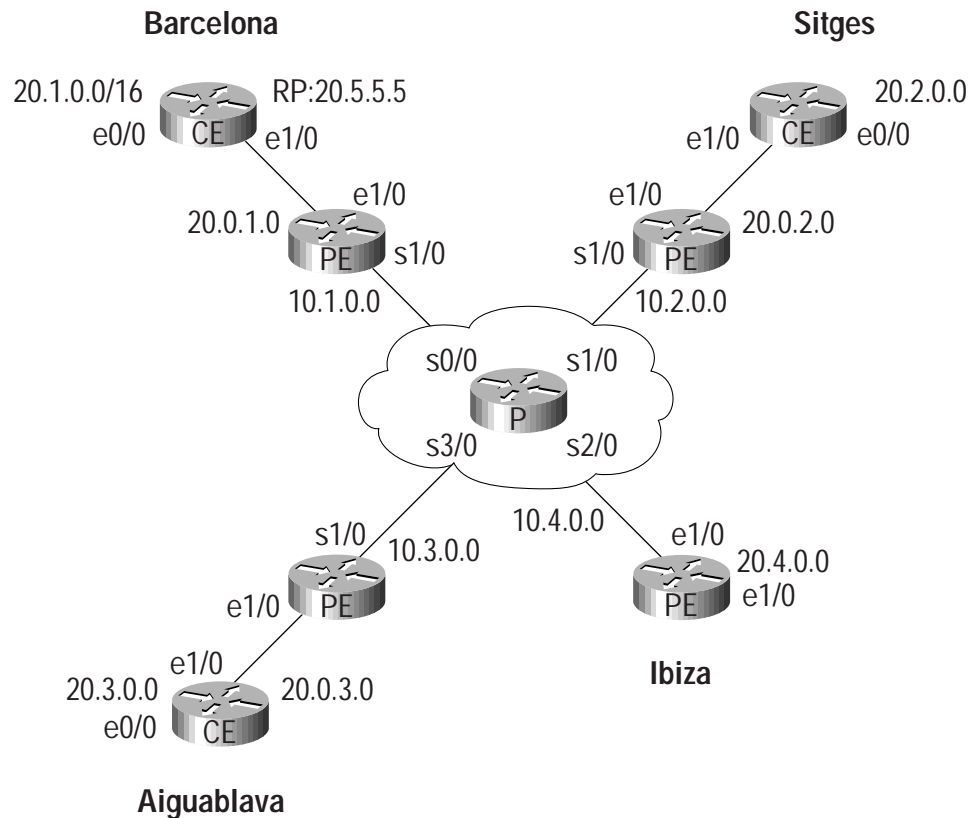
Configuring the Provider Network

Throughout this document the following topology will be used. It describes a sample service provider network providing an MVPN service to VPN customer 'catalunya'.

Figure 1



Network Topology



Step 1. Choosing the PIM mode for the provider network:

Cisco recommends PIM-SSM as the protocol in the core. For source-discovery a new attribute is added to BGP, so no additional configuration is required.

A new RD type is used to advertise the source of the MDT together with the MDT group address. For details on the implementation see Appendix: x, PIM SM has been the most widely deployed multicast protocol and has been used for both sparsely and densely populated application requirements. PIM SSM, though newer, is based upon PIM SM. Without the initial Shared tree and subsequent cutover to the Shortest Path Tree, either PIM SSM or PIM SM is suitable for the default MDT.

When Bi-dir PIM support is eventually available on all relevant hardware, it will be the obvious recommendation for the default MDT.

For the Data MDT, either PIM SM or PIM SSM is suitable.

PIM SSM is simpler to deploy than PIM SM. It does not require a Rendezvous point, and the Provider network is a known and stable group of multicast devices. Cisco recommends the use of PIM SSM for Provider core deployment

Step 2. Choosing the VPN group addresses used inside the provider network:



In Step 1, PIM-SSM was selected. The default PIM-SSM range is 232/8; however, this address range is designed for global use in the Internet. For use within a private domain, the use of an address out of the administratively scoped multicast range, 239/8, is recommended (RFC2365). Using this private address range makes it simpler to filter on boundary routers.

Cisco recommends using 239.232/16, as this address range is easily recognizable as both a private address and a SSM address by using 232 in the second octet.

In the design discussed in this document, the range will be divided for default-MDT and data-MDT. Data-MDT will be discussed elsewhere in this document. Default-MDTs will use 239.232.0.0-239.232.0.256 and Data-MDTs will use 239.232.1.0-239.232.255.255. This address range will provide support for up to 255 MVRFs per PE router.

Step 3. Configuring the provider network for PIM-SSM

The following commands need to be configured to enable a basic PIM-SSM service.

On all P and PE routers configure globally:

```
ip multicast-routing
access-list 1 permit 239.232.0.0 0.0.255.255
ip pim ssm range 1
```

On all P interfaces and PE interfaces facing the core configure:

```
ip pim sparse-mode
```

On the PE routers configure on the loopback interface used to source the BGP session

```
ip pim sparse-mode
```

Step 4. Configuring the MDT on the VRF

To configure multicast routing on the VRF, configure on all PE routers for the VRF catalunya:

```
mdt default 239.232.0.0
```

To enable multicast routing for this VRF configure:

```
ip multicast-routing vrf catalunya
```

Sample provider network configuration



Below the configuration on PE_BARCELONA with only the relevant multicast configurations after completion of the steps above:

```
ip vrf catalunya
  rd 1:1
  route-target export 1:1
  route-target import 1:1
  mdt default 239.232.0.0
!
ip multicast-routing
ip multicast-routing vrf catalunya
!
interface Loopback0
  ip address 10.0.0.1 255.255.255.255
  ip pim sparse-mode
!
interface Serial 1/0
  ip address 10.1.0.1 255.255.255.0
  ip pim sparse-mode
  tag-switching ip
!
ip pim ssm range 1
!
access-list 1 permit 239.232.0.0 0.0.255.255
```

Choosing the Pim Mode for the VPN

The PIM mode inside the VPN depends on what the VPN customer is using. Cisco provides automatic discovery of the group-mode used inside the VPN via auto-rp or bsr, which requires no additional configuration.

Optionally, a provider may choose to provide the RP for the customer by configuring the PE router as an RP inside the VPN.

In the topology discussed in this document, the VPN customer is providing the RP service and the PE routers will automatically learn the Group to RP mapping via Auto-RP.

Step 5. Configuring the pim mode inside the VPN

Configure all PE-CE interfaces for sparse-dense-mode which will make sure that either auto-rp or bsr messages are received and forwarded allowing the PE to learn the group to rp mapping inside the vpn.

Configure on all customer facing interfaces:

```
ip pim sparse-dense-mode
```



Sample Customer Facing Network Configuration

```

!
interface Ethernet0/0
 ip vrf forwarding catalunya
 ip address 20.0.1.1 255.255.255.0
 ip pim sparse-dense-mode
!

```

Verifying the Network

When the five steps above have been configured, use the following command to verify that all has been setup properly:

```

show ip pim mdt bgp
show ip bgp vpnv4 all
show ip mroute
show ip pim neighbors
show ip pim vrf catalunya neighbors
show ip pim vrf catalunya rp mapping

```

Step 1. Verify BGP updates

BGP provides for source discovery when SSM is used, which is known as a BGP-MDT update. Use 'show ip pim mdt bgp' to verify that all BGP-MDT updates have been received correctly on the PE routers.

```

PE_BARCELONA#show ip pim mdt bgp
Peer (Route Distinguisher + IPv4)                Next Hop
MDT group 239.232.0.0
2:1:1:10.0.0.2                                    10.0.0.2
2:1:1:10.0.0.3                                    10.0.0.3
2:1:1:10.0.0.4                                    10.0.0.4

```

2:1:1 indicates the RD-type (2) and RD (1:1) associated with this update.

The remaining part is the address used to source the BGP session.

Alternatively, 'show ip bgp vpnv4 all' can be used.

```

PE_BARCELONA#show ip bgp vpnv4 all
BGP table version is 24, local router ID is 10.0.0.1
Status codes:  s suppressed, d damped, h history, * valid, > best, i - internal,
                r RIB-failure, S Stale
Origin codes:  i - IGP, e - EGP, ? - incomplete

```

Network	Next Hop	Metric	LocPrf	Weight Path
Route Distinguisher: 1:1 (default for vrf catalunya)				
*> 20.0.1.0/24	0.0.0.0	0		32768 ?
*>i20.0.2.0/24	10.0.0.2	0	100	0 ?
*>i20.0.3.0/24	10.0.0.3	0	100	0 ?
*> 20.1.0.0/22	20.0.1.2	0		32768 ?
*> 20.1.0.0/16	20.0.1.2	0		32768 ?
*>i20.2.0.0/24	10.0.0.2	1	100	0 ?
*>i20.3.0.0/24	10.0.0.3	1	100	0 ?
*>i20.4.0.0/24	10.0.0.4	0	100	0 ?
*> 20.5.5.5/32	20.0.1.2	1		32768 ?
Route Distinguisher: 2:1:1				
*> 10.0.0.1/32	0.0.0.0			0 ?
*>i10.0.0.2/32	10.0.0.2	0	100	0 ?
*>i10.0.0.3/32	10.0.0.3	0	100	0 ?
*>i10.0.0.4/32	10.0.0.4	0	100	0 ?



Step 2. Verify the global mroute table

Use 'show ip mroute <mdt-group-address>' to verify that there is a (Source,Group) entry for each PE router. As PIM-SSM is used, the source is the loopback address used to source the BGP session and the Group is the MDT address configured. Without traffic, only default-MDT entries will be visible.

```
PE_BARCELONA#show ip mroute 239.232.0.0
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
T - SPT-bit set, J - Join SPT, M - MSDP created entry,
X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(10.0.0.1, 239.232.0.0), 00:18:40/00:03:14, flags: sTZ
Incoming interface: Loopback0, RPF nbr 0.0.0.0
Outgoing interface list:
Serial 1/0, Forward/Sparse, 00:17:53/00:02:31

(10.0.0.2, 239.232.0.0), 00:17:52/00:02:44, flags: sTIZ
Incoming interface: Ethernet0/0, RPF nbr 10.1.0.2
Outgoing interface list:
MVRF catalunya, Forward/Sparse, 00:17:52/00:00:00

(10.0.0.3, 239.232.0.0), 00:17:47/00:02:44, flags: sTIZ
Incoming interface: Ethernet0/0, RPF nbr 10.1.0.2
Outgoing interface list:
MVRF catalunya, Forward/Sparse, 00:17:47/00:00:00

(10.0.0.4, 239.232.0.0), 00:17:46/00:02:44, flags: sTIZ
Incoming interface: Ethernet0/0, RPF nbr 10.1.0.2
Outgoing interface list:
MVRF catalunya, Forward/Sparse, 00:17:46/00:00:00
```



Verify that the 's' flag is set on each (S,G) entry, which indicates that this group is used in ssm mode. Verify that the 'Z' flag is set indicating that this PE router is a leaf of the multicast tunnel. When the router is a 'leaf' of a multicast tunnel, it has to do additional lookups to determine which MVRF to forward this traffic to, as it is basically a receiver for this traffic.

Verify the I flag is set for the remote PE(S,G) entry. This flag indicates that the router understands it is joining an SSM group. It is as though an IGMPv3 host had requested to join that particular channel.

Step 3. Verify PIM neighbors in the global table

Use the 'show ip pim neighbors' command on all PE and P routers to verify that the pim neighbors are setup properly in the global table.

```
PE_BARCELONA#show ip pim neighbor
PIM Neighbor Table
Neighbor          Interface      Uptime/Expires      Ver   DR
Address
10.1.0.2          Serial 1/0     00:18:36/00:01:21   v2    1 / S
```

The example above shows that PE_BARCELONA has correctly setup a PIM neighborhood in the global table with the P router.

Step 4. Verify PIM neighbors inside the VPN

Use 'show ip pim vrf catalunya neighbors' on all PE routers to verify that the CE router is seen as a PIM neighbor and the remote-PE routers are seen as a pim neighbor over the tunnel.

```
PE_BARCELONA#show ip pim vrf catalunya neighbor
PIM Neighbor Table
Neighbor          Interface      Uptime/Expires      Ver   DR
Address
20.0.1.2          Ethernet0/0    00:18:30/00:01:27   v2    1 / DR
10.0.0.3          Tunnel0        00:17:40/00:01:18   v2    1 /
10.0.0.4          Tunnel0        00:17:40/00:01:19   v2    1 / DR
10.0.0.2          Tunnel0        00:17:40/00:01:19   v2    1 /
```

There is correctly a PIM neighbor with the CE router on interface Ethernet 1/0, and all remote PE routers are also seen as PIM neighbors over the tunnel.

Step 5. Verify the VPN Group to RP mapping



Use 'show ip pim vrf catalunya rp mapping' to verify that the PE router correctly learned the Group to RP mapping information from the VPN.

```
PE_BARCELONA#show ip pim vrf catalunya rp map
PIM Group-to-RP Mappings

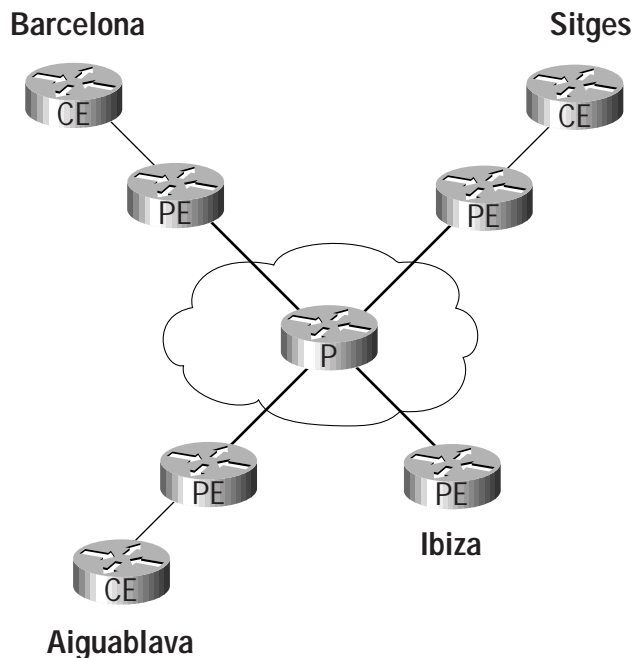
Group(s) 224.0.0.0/4
  RP 20.5.5.5 (?), v2v1
    Info source: 20.5.5.5 (?), elected via Auto-RP
    Uptime: 00:10:34, expires: 00:02:24
```

The PE router has correctly learned the Group to RP mapping, which is used inside the VPN. Auto-RP is used here inside the VPN.

When all the above has been successfully verified, Figure 2 presents a conceptual overview showing the default-MDT reaching all PE routers with the multicast replication being done in the core of the provider network.

With only a default-MDT configured, traffic will go to all PE routers, regardless of whether they want to receive the traffic.

Figure 2
Only a default-MDT



Optimizing Traffic Forwarding: Data-MDT

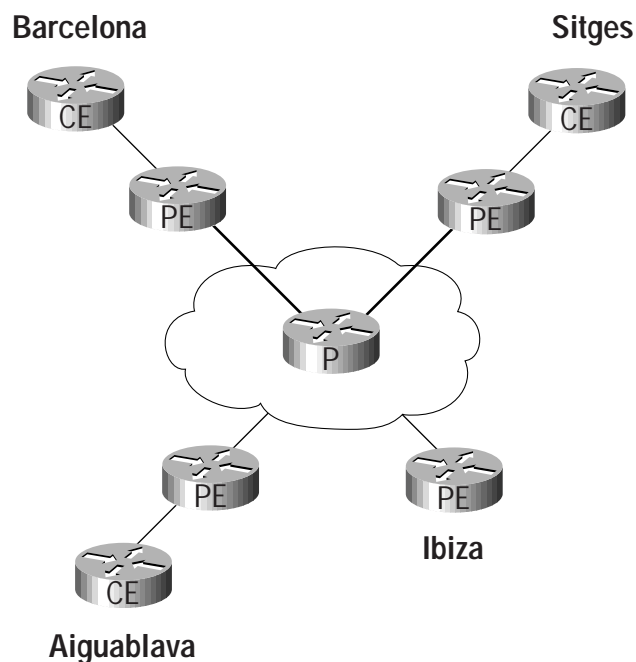
To optimize traffic forwarding, the concept of data-MDT has been introduced. This is a multicast tree that is constructed on demand. The conditions to create a data-MDT are based upon traffic-load threshold measured in kbps and/or an access-list specifying certain sources inside the VPN. A data-MDT will be created only by the PE that has the source connected to its site.



The data-MDT conditions do not have to be configured; however, if there are no conditions set then for each (S,G) inside the VPN, then a data-MDT will be created. This data-MDT will require resources from the router, so it is not recommended to create a one merely because a source exists. A non zero threshold is recommended, as this will require an active source to trigger the creation of the Data MDT. The maximum number of MVRF is 256.

The following topology shows a data-mdt being setup for a source that is behind PE_BARCELONA and a receiver that is behind PE_SITGES. Note that no traffic will be flowing towards PE_AIGUABLAVA and PE_IBIZA.

Figure 3
Data-MDT setup



Step 1. Configuring the data-mdt

Configure the data MDT under the VRF. Use one of the ranges as defined in Step 2 of “Configuring the provider network”. A maximum of 256 addresses is currently allowed per VRF. This is an implementation choice, not a protocol limitation.

As SSM is used, the data-MDT address-range may be the same on all PE routers for the same VPN. Use an inverse-mask to specify the number of addresses used for the data-MDT.

```
!  
ip vrf catalunya  
  mdt data 239.232.1.0 0.0.0.255 threshold 1  
!
```

Step 2. Configuring data-mdt management

As there are a limited number of addresses available for the data-MDT, addresses may be re-used if this limit is reached. This re-use will occur based on a “ref-count”, meaning the data-MDT addresses that have been used least will be re-used. Re-use may result in sub-optimal forwarding but will ensure stability in the provider core.



A configuration command has been added to manage this, and to verify data-MDT reuse. Configuration of this command means that a syslog message will be generated when a data-MDT is reused. An SNMP trap will then be generated.

Configure under the vrf the following command

```
!  
ip vrf catalunya  
  mdt log-reuse
```

Verifying Correct Data-MDT Operation

Data-MDTs will create an mroute-entry in the global table. There are also some specific commands about verifying functionality by sending and receiving PE router.

Step 1. Verify the sending PE router

Use 'show ip pim vrf catalunya mdt send' on the sending PE router to verify the setup of a data-mdt.

```
PE_BARCELONA#show ip pim vrf catalunya mdt send  
MDT-data send list for VRF: catalunya  
  (source, group)          MDT-data group          ref_count  
  (20.1.0.44,              239.0.0.1)              239.232.1.0 1
```

Data-MDT 239.232.1.0 is used for the source.group pair (20.1.0.44,239.0.0.1) inside the VPN. The ref_count of 1 shows that data-mdt 239.232.1.0 is only used one time.

Use 'show ip mroute' to verify that the data-mdt has correctly created a mroute state in the global table.

```
PE_BARCELONA#show ip mroute  
IP Multicast Routing Table  
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,  
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,  
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,  
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,  
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,  
       Y - Joined MDT-data group, y - Sending to MDT-data group  
Outgoing interface flags: H - Hardware switched  
Timers: Uptime/Expires  
Interface state: Interface, Next-Hop or VCD, State/Mode  
  
(10.0.0.1, 239.232.1.0), 00:11:10/00:03:23, flags: sTZ  
Incoming interface: Loopback0, RPF nbr 0.0.0.0  
Outgoing interface list:  
Ethernet0/0, Forward/Sparse, 00:11:10/00:03:03
```

Verify the correct setting of the Z flag



Use 'show ip mroute vrf catalunya' to verify that the source.group pair inside the VPN is correctly sending to the data-MDT.

```
PE_BARCELONA#show ip mroute vrf catalunya
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.0.0.1), 00:11:11/00:03:04, RP 20.5.5.5, flags: S
Incoming interface: Ethernet0/0, RPF nbr 20.0.1.2
Outgoing interface list:
  Tunnel0, Forward/Sparse-Dense, 00:11:11/00:03:04

(20.1.0.44, 239.0.0.1), 00:11:10/00:03:24, flags: Ty
Incoming interface: Ethernet0/0, RPF nbr 20.0.1.2
Outgoing interface list:
  Tunnel0, Forward/Sparse-Dense, 00:11:10/00:03:04
```

Note the little 'y' flag. This indicates that this group is sending on a data-MDT.

Step 2. Verify the receiving PE router

Use 'show ip pim vrf catalunya mdt receive detail' on the receiving PE router to verify that this router is receiving on a data-mdt.

```
PE_SITGES#show ip pim vrf catalunya mdt receive detail
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group

Joined MDT-data [group : source] uptime/expires for VRF: catalunya
[239.232.1.0 : 10.0.0.1] 00:11:20/00:02:35
(20.1.0.44, 239.0.0.1), 00:11:20/00:03:26/00:02:35, OIF count: 1, flags: TY
```

Note the big 'Y' flag to indicate that we're receiving on this data-MDT.



Use 'show ip mroute' on the receiving PE router to verify that the data-mdt created state inside the global table and that the Z flag is set and the outgoing interface is pointing to the correct MVRF.

```
PE_SITGES#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(10.0.0.1, 239.232.1.0), 00:11:20/00:02:56, flags: sTIZ
Incoming interface: Serial 1/0/0, RPF nbr 10.2.0.2
Outgoing interface list:
    MVRF catalunya, Forward/Sparse, 00:11:20/00:00:00
```

Use 'show ip mroute vrf catalunya' to verify the correct state inside the VPN.

Again verify the big 'Y' flag to indicate we're receiving on a data-MDT.

```
PE_SITGES#show ip mroute vrf catalunya
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.0.0.1), 00:11:20/stopped, RP 20.5.5.5, flags: S
Incoming interface: Tunnel0, RPF nbr 10.0.0.1
Outgoing interface list:
    Ethernet0/0, Forward/Sparse-Dense, 00:11:20/00:02:51

(20.1.0.44, 239.0.0.1), 00:11:20/00:03:26, flags: TY
Incoming interface: Tunnel0, RPF nbr 10.0.0.1
Outgoing interface list:
    Ethernet0/0, Forward/Sparse-Dense, 00:11:20/00:02:51
```

Step 3. Verify data-mdt management

Used on the sending PE router a syslog message will be printed in the event of a data-MDT reuse. These messages are rate-limited to maximum one per minute.

```
1d02h: %MDT-5-DATA_MDT_REUSED: Data MDT 239.232.1.0 is reused in VRF catalunya
```

There is an additional show command that illustrates the amount of re-uses that occurred over a certain interval specified in minutes.



Example:

```
PE_BARCELONA# show ip pim vrf catalunya mdt history interval 60
MDT-data send history of VRF - catalunya for the past 60 minutes
MDT-data group      Number of reuse
 239.232.1.14       1
 239.232.1.15       1
```

This corresponds with the ref-count in the 'show ip pim mdt vrf catalunya send' command

```
PE_BARCELONA#show ip pim vrf catalunya mdt send
MDT-data send list for VRF: catalunya
 (source, group)    MDT-data group  ref_count
 (20.1.0.5,         239.0.0.1)      239.232.1.14 2
 (20.1.0.6,         239.0.0.1)      239.232.1.15 2
```

Additional Information

All multicast protocols can now operate in the context of a VRF. The configuration syntax stays the same with the exception of the additional 'vrf' keyword.

Example:

```
ip msdp peer a.b.c.d
```

When configured for a vrf becomes:

```
ip msdp vrf catalunya peer a.b.c.d
```

The same rules apply for show and debug commands

Example:

```
Show ip igmp group
```

When used for a vrf becomes:

```
show ip igmp vrf catalunya group
```

Example output:

```
PE_IBIZA#show ip igmp vrf catalunya group
IGMP Connected Group Membership
Group Address      Interface      Uptime        Expires        Last Reporter
239.0.0.1          Ethernet 1/0   00:18:59     00:02:03     20.4.0.10
```

Configurations from all Relevant Routers

Find below the configurations of all PE routers, CE_Barcelona, and the P router.



PE Barcelona

```
!  
hostname PE_BARCELONA  
!  
logging queue-limit 100  
!  
clock timezone CET 1  
ip subnet-zero  
ip cef  
no ip domain lookup  
!  
ip vrf catalunya  
  rd 1:1  
  route-target export 1:1  
  route-target import 1:1  
  mdt default 239.232.0.0  
  mdt data 239.232.1.0 0.0.0.255  
  mdt log-reuse  
!  
ip multicast-routing  
ip multicast-routing vrf catalunya  
mpls ldp logging neighbor-changes  
!  
!  
interface Loopback0  
  ip address 10.0.0.1 255.255.255.255  
  ip pim sparse-mode  
!  
interface Ethernet0/0  
  ip vrf forwarding catalunya  
  ip address 20.0.1.1 255.255.255.0  
  ip pim sparse-dense-mode  
!  
interface Serial1/0  
  ip address 10.1.0.1 255.255.255.0  
  ip pim sparse-mode  
  encapsulation ppp  
  tag-switching ip  
!  
router eigrp 1  
  network 10.0.0.0  
  auto-summary  
!  
router rip  
  version 2  
  !  
  address-family ipv4 vrf catalunya  
  version 2  
  redistribute bgp 1 metric 1  
  network 20.0.0.0  
  no auto-summary  
  exit-address-family  
!  
router bgp 1  
  no synchronization  
  bgp log-neighbor-changes
```



```
neighbor 10.0.0.2 remote-as 1
neighbor 10.0.0.2 update-source Loopback0
neighbor 10.0.0.3 remote-as 1
neighbor 10.0.0.3 update-source Loopback0
neighbor 10.0.0.4 remote-as 1
neighbor 10.0.0.4 update-source Loopback0
no auto-summary
!
address-family vpnv4
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 send-community both
neighbor 10.0.0.3 activate
neighbor 10.0.0.3 send-community both
neighbor 10.0.0.4 activate
neighbor 10.0.0.4 send-community both
exit-address-family
!
address-family ipv4 vrf catalunya
redistribute static
redistribute rip
no auto-summary
no synchronization
exit-address-family
!
ip classless
ip route vrf catalunya 20.1.0.0 255.255.0.0 20.0.1.2
ip route vrf catalunya 20.1.0.0 255.255.252.0 20.0.1.2
no ip http server
!
ip pim ssm range 1
!
access-list 1 permit 239.232.0.0 0.0.255.255
!
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  login
!
!
end
```



PE Sitges

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname PE_SITGES  
!  
!  
ip subnet-zero  
ip cef  
no ip domain-lookup  
ip vrf catalunya  
  rd 1:1  
  route-target export 1:1  
  route-target import 1:1  
  mdt default 239.232.0.0  
  mdt data 239.232.1.0 0.0.0.255 threshold 1  
  mdt log-reuse  
!  
ip multicast-routing  
ip multicast-routing vrf catalunya  
mpls ldp logging neighbor-changes  
no mpls traffic-eng auto-bw timers frequency 0  
!  
!  
!  
interface Loopback0  
  ip address 10.0.0.2 255.255.255.255  
  no ip directed-broadcast  
  ip pim sparse-mode  
!  
interface Ethernet0/0  
  ip vrf forwarding catalunya  
  ip address 20.0.2.1 255.255.255.0  
  no ip directed-broadcast  
  ip pim sparse-dense-mode  
!  
interface Serial1/0  
  ip address 10.2.0.1 255.255.255.0  
  no ip directed-broadcast  
  ip pim sparse-mode  
  encapsulation ppp  
  tag-switching ip  
!  
router eigrp 1  
  network 10.0.0.0  
!  
router rip  
  version 2  
  !  
  address-family ipv4 vrf catalunya  
  version 2  
  redistribute bgp 1 metric 1  
  network 20.0.0.0
```



```
no auto-summary
exit-address-family
!
router bgp 1
no synchronization
bgp log-neighbor-changes
neighbor 10.0.0.1 remote-as 1
neighbor 10.0.0.1 update-source Loopback0
neighbor 10.0.0.3 remote-as 1
neighbor 10.0.0.3 update-source Loopback0
neighbor 10.0.0.4 remote-as 1
neighbor 10.0.0.4 update-source Loopback0
no auto-summary
!
address-family vpnv4
neighbor 10.0.0.1 activate
neighbor 10.0.0.1 send-community both
neighbor 10.0.0.3 activate
neighbor 10.0.0.3 send-community both
neighbor 10.0.0.4 activate
neighbor 10.0.0.4 send-community both
exit-address-family
!
address-family ipv4 vrf catalunya
redistribute rip
no auto-summary
no synchronization
exit-address-family
!
ip classless
!
ip pim ssm range 1
!
!
access-list 1 permit 239.232.0.0 0.0.255.255
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  login
!
end
```



PE Aiguablava

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname PE_AIGUABLAVA  
!  
!  
ip subnet-zero  
ip cef  
no ip domain-lookup  
ip vrf catalunya  
  rd 1:1  
  route-target export 1:1  
  route-target import 1:1  
  mdt default 239.232.0.0  
  mdt data 239.232.1.0 0.0.0.255 threshold 1  
  mdt log-reuse  
!  
ip multicast-routing  
ip multicast-routing vrf catalunya  
mpls ldp logging neighbor-changes  
no mpls traffic-eng auto-bw timers frequency 0  
!  
!  
!  
interface Loopback0  
  ip address 10.0.0.3 255.255.255.255  
  no ip directed-broadcast  
  ip pim sparse-mode  
!  
interface Ethernet0/0  
  ip vrf forwarding catalunya  
  ip address 20.0.3.1 255.255.255.0  
  no ip directed-broadcast  
  ip pim sparse-dense-mode  
!  
interface Serial1/0  
  ip address 10.3.0.1 255.255.255.0  
  no ip directed-broadcast  
  ip pim sparse-mode  
  encapsulation ppp  
  tag-switching ip  
!  
router eigrp 1  
  network 10.0.0.0  
!  
router rip  
  version 2  
  !  
  address-family ipv4 vrf catalunya  
  version 2  
  redistribute bgp 1 metric 1  
  network 20.0.0.0
```



```
no auto-summary
exit-address-family
!
router bgp 1
no synchronization
bgp log-neighbor-changes
neighbor 10.0.0.1 remote-as 1
neighbor 10.0.0.1 update-source Loopback0
neighbor 10.0.0.2 remote-as 1
neighbor 10.0.0.2 update-source Loopback0
neighbor 10.0.0.4 remote-as 1
neighbor 10.0.0.4 update-source Loopback0
no auto-summary
!
address-family vpnv4
neighbor 10.0.0.1 activate
neighbor 10.0.0.1 send-community both
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 send-community both
neighbor 10.0.0.4 activate
neighbor 10.0.0.4 send-community both
exit-address-family
!
address-family ipv4 vrf catalunya
redistribute rip
no auto-summary
no synchronization
exit-address-family
!
ip classless
!
ip pim ssm range 1
!
!
access-list 1 permit 239.232.0.0 0.0.255.255
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  login
!
end
```



PE Ibiza

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname PE_IBIZA  
!  
!  
ip subnet-zero  
ip cef  
no ip domain-lookup  
ip vrf catalunya  
  rd 1:1  
  route-target export 1:1  
  route-target import 1:1  
  mdt default 239.232.0.0  
  mdt data 239.232.1.0 0.0.0.255 threshold 1  
  mdt log-reuse  
!  
ip multicast-routing  
ip multicast-routing vrf catalunya  
mpls ldp logging neighbor-changes  
no mpls traffic-eng auto-bw timers frequency 0  
!  
!  
!  
interface Loopback0  
  ip address 10.0.0.4 255.255.255.255  
  no ip directed-broadcast  
  ip pim sparse-mode  
!  
interface Ethernet0/0  
  ip vrf forwarding catalunya  
  ip address 20.4.0.1 255.255.255.0  
  no ip directed-broadcast  
  ip pim sparse-dense-mode  
!  
interface Serial1/0  
  ip address 10.4.0.1 255.255.255.0  
  no ip directed-broadcast  
  ip pim sparse-mode  
  encapsulation ppp  
  tag-switching ip  
!  
router eigrp 1  
  network 10.0.0.0  
!  
router rip  
  version 2  
  !  
  address-family ipv4 vrf catalunya  
  version 2  
  redistribute bgp 1 metric 1  
  network 20.0.0.0
```



```
no auto-summary
exit-address-family
!
router bgp 1
no synchronization
bgp log-neighbor-changes
neighbor 10.0.0.1 remote-as 1
neighbor 10.0.0.1 update-source Loopback0
neighbor 10.0.0.2 remote-as 1
neighbor 10.0.0.2 update-source Loopback0
neighbor 10.0.0.3 remote-as 1
neighbor 10.0.0.3 update-source Loopback0
no auto-summary
!
address-family vpnv4
neighbor 10.0.0.1 activate
neighbor 10.0.0.1 send-community both
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 send-community both
neighbor 10.0.0.3 activate
neighbor 10.0.0.3 send-community both
exit-address-family
!
address-family ipv4 vrf catalunya
redistribute rip
no auto-summary
no synchronization
exit-address-family
!
ip classless
!
ip pim ssm range 1
!
!
access-list 1 permit 239.232.0.0 0.0.255.255
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  login
!
end
```



CE Barcelona

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname CE_BARCELONA  
!  
!  
ip subnet-zero  
ip cef  
no ip domain-lookup  
ip multicast-routing  
mpls ldp logging neighbor-changes  
no mpls traffic-eng auto-bw timers frequency 0  
!  
!  
!  
interface Loopback0  
 ip address 20.5.5.5 255.255.255.255  
 no ip directed-broadcast  
 ip pim sparse-dense-mode  
!  
interface Ethernet0/0  
 ip address 20.1.0.1 255.255.0.0  
 no ip directed-broadcast  
 ip pim sparse-dense-mode  
!  
interface Ethernet1/0  
 ip address 20.0.1.2 255.255.252.0  
 no ip directed-broadcast  
 ip pim sparse-dense-mode  
!  
router rip  
 version 2  
 network 20.0.0.0  
!  
ip classless  
!  
ip pim send-rp-announce Loopback0 scope 64  
ip pim send-rp-discovery Loopback0 scope 64  
!  
!  
!  
line con 0  
  exec-timeout 0 0  
line aux 0  
line vty 0 4  
  login  
!  
end
```

P Router

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P_ROUTER
!
!
ip subnet-zero
ip cef
no ip domain-lookup
ip multicast-routing
mpls ldp logging neighbor-changes
no mpls traffic-eng auto-bw timers frequency 0
!
!
!
interface Serial0/0
 ip address 10.1.0.2 255.255.255.0
 no ip directed-broadcast
 ip pim sparse-mode
 encapsulation ppp
 tag-switching ip
!
interface Serial1/0
 ip address 10.2.0.2 255.255.255.0
 no ip directed-broadcast
 ip pim sparse-mode
 encapsulation ppp
 tag-switching ip
!
interface Serial2/0
 ip address 10.4.0.2 255.255.255.0
 no ip directed-broadcast
 ip pim sparse-mode
 encapsulation ppp
 tag-switching ip
!
interface Serial3/0
 ip address 10.3.0.2 255.255.255.0
 no ip directed-broadcast
 ip pim sparse-mode
 encapsulation ppp
 tag-switching ip
!
router eigrp 1
 network 10.0.0.0
!
ip classless
!
ip pim ssm range 1
!
!
access-list 1 permit 239.232.0.0 0.0.255.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992-2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0304R) 203115.A/ETMG_07/03