IP Multicast: Multicast Legacy Technologies, Cisco IOS Release 12.2SY

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Last Updated: July 18, 2011

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Configuring IP Multicast over ATM Point-to-Multipoint VCs

This module describes how to configure IP multicast over ATM point-to-multipoint virtual circuits (VCs). This feature dynamically creates ATM point-to-multipoint switched virtual circuits (SVCs) to handle IP multicast traffic more efficiently. It can enhance router performance and link utilization because packets are not replicated and sent multiple times over the ATM interface.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IP Multicast over ATM Point-to-Multipoint VCs

- You must have IP multicast routing and PIM sparse mode configured. This feature does not work with PIM dense mode.
- You must have ATM configured for multipoint signaling.
- You should understand the concepts in the “ IP Multicast Technology Overview ” module.

Information About IP Multicast over ATM Point-to-Multipoint VCs

PIM Nonbroadcast Multiaccess

Protocol Independent Multicast (PIM) nonbroadcast multiaccess (NBMA) mode allows the software to replicate packets for each neighbor on the NBMA network. Traditionally, the software replicates multicast and broadcast packets to all broadcast configured neighbors. This action might be inefficient when not all neighbors want packets for certain multicast groups. NBMA mode enables you to reduce bandwidth on links leading into the NBMA network, and to reduce the number of CPU cycles in switches and attached neighbors.

It is appropriate to configure PIM NBMA mode on ATM, Frame Relay, Switched Multimegabit Data Service (SMDS), PRI ISDN, or X.25 networks only, especially when these media do not have native multicast available. Do not use PIM NBMA mode on multicast-capable LANs (such as Ethernet or FDDI).

You should use PIM sparse mode with this feature. Therefore, when each Join message is received from NBMA neighbors, PIM stores each neighbor IP address and interface in the outgoing interface list for the group. When a packet is destined for the group, the software replicates the packet and unicasts (data-link unicasts) it to each neighbor that has joined the group.

Consider the following two factors before enabling PIM NBMA mode:

- If the number of neighbors grows, the outgoing interface list gets large, which costs memory and replication time.
- If the network (Frame Relay, SMDS, or ATM) supports multicast natively, you should use it so that replication is performed at optimal points in the network.

IP Multicast over ATM Point-to-Multipoint VCs

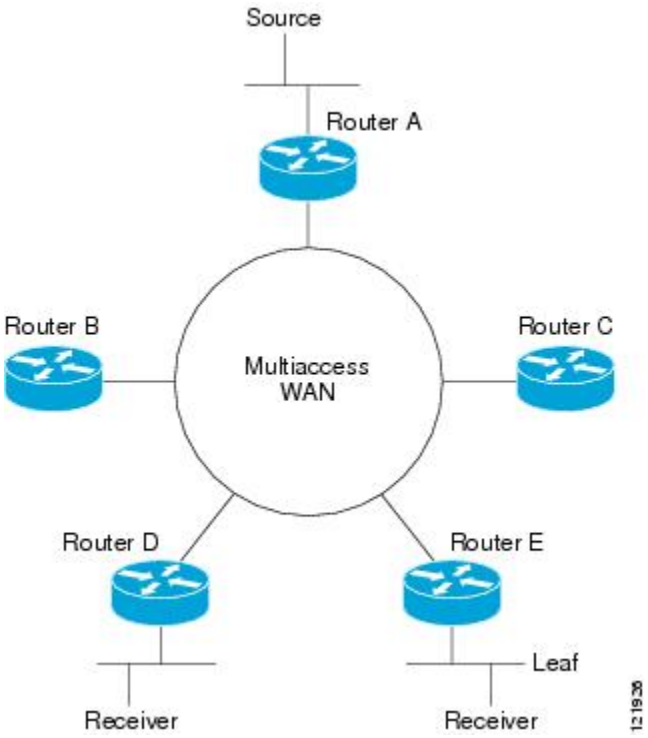
IP Multicast over ATM Point-to-Multipoint VCs is a feature that dynamically creates ATM point-to-multipoint switched virtual circuits (SVCs) to handle IP multicast traffic more efficiently.

This feature can enhance router performance and link utilization because packets are not replicated and sent multiple times over the ATM interface.

Traditionally, over NBMA networks, Cisco routers would perform a pseudobroadcast to get broadcast or multicast packets to all neighbors on a multiaccess network. For example, assume in the figure that Routers A, B, C, D, and E were running the Open Shortest Path First (OSPF) protocol. Router A must deliver to Routers D and E. When Router A sends an OSPF Hello packet, the data link layer replicates the Hello

packet and sends one to each neighbor (this procedure is known as pseudobroadcast), which results in four copies being sent over the link from Router A to the multiaccess WAN.

Figure 1



With the advent of IP multicast, where high-rate multicast traffic can occur, the pseudobroadcast approach does not scale. Furthermore, in the preceding example, Routers B and C would get data traffic they do not need. To handle this problem, PIM can be configured in NBMA mode using the **ip pim nbma-mode** command. PIM in NBMA mode works only for sparse mode groups. Configuring PIM in NBMA mode would allow only Routers D and E to get the traffic without distributing to Routers B and C. However, two copies are still delivered over the link from Router A to the multiaccess WAN.

If the underlying network supported multicast capability, the routers could handle this situation more efficiently. If the multiaccess WAN were an ATM network, IP multicast could use multipoint VCs.

To configure IP multicast using multipoint VCs, Routers A, B, C, D, and E in the figure must run PIM sparse mode. If the Receiver directly connected to Router D joins a group and Router A is the PIM RP, the following sequence of events occurs:

1. Router D sends a PIM Join message to Router A.
2. When Router A receives the PIM join, it sets up a multipoint VC for the multicast group.
3. Later, when the Receiver directly connected to Router E joins the same group, Router E sends a PIM Join message to Router A.
4. Router A will see there is a multipoint VC already associated with the group, and will add Router E to the existing multipoint VC.
5. When the Source sends a data packet, Router A can send a single packet over its link that gets to both Router D and Router E. The replication occurs in the ATM switches at the topological diverging point from Router A to Router D and Router E.

If a host sends an IGMP report over an ATM interface to a router, the router adds the host to the multipoint VC for the group.

This feature can also be used over ATM subinterfaces.

Idling Policy for ATM VCs Created by PIM

An idling policy uses the **ip pim vc-count** command to limit the number of VCs created by PIM. When the router stays at or below the number configured, no idling policy is in effect. When the next VC to be opened will exceed the value, an idling policy is exercised. An idled VC does not mean that the multicast traffic is not forwarded; the traffic is switched to VC 0. VC 0 is the broadcast VC that is open to all neighbors listed in the map list. The name VC 0 is unique to PIM and the mroute table.

How the Idling Policy Works

The idling policy works as follows:

- The only VCs eligible for idling are those with a current 1-second activity rate less than or equal to the value configured by the **ip pim minimum-vc-rate** interface configuration command on the ATM interface. Activity level is measured in packets per second (pps).
- The VC with the least amount of activity below the configured **ip pim minimum-vc-rate** pps rate is idled.
- If the **ip pim minimum-vc-rate** command is not configured, all VCs are eligible for idling.
- If other VCs are at the same activity level, the VC with the highest fanout (number of leaf routers on the multipoint VC) is idled.
- The activity level is rounded to three orders of magnitude (less than 10 pps, 10 to 100 pps, and 100 to 1000 pps). Therefore, a VC that has 40 pps activity and another that has 60 pps activity are considered to have the same rate, and the fanout count determines which one is idled. If the first VC has a fanout of 5 and the second has a fanout of 3, the first one is idled.
- Idling a VC means releasing the multipoint VC that is dedicated for the multicast group. The traffic of the group continues to be sent; it is moved to the static map VC. Packets will flow over a shared multipoint VC that delivers packets to all PIM neighbors.
- If all VCs have a 1-minute rate greater than the pps value, the new group (that exceeded the **ip pim vc-count** *number*) will use the shared multipoint VC.

Keeping VCs from Idling

By default, all VCs are eligible for idling. You can configure a minimum rate required to keep VCs from being idled.

How to Configure IP Multicast over ATM Point-to-Multipoint VCs

Configuring IP Multicast over ATM Point-to-Multipoint VCs

Perform this task to configure IP multicast over ATM point-to-multipoint VCs. All of the steps in the task can be used in an ATM network. This feature can also be used over ATM subinterfaces. PIM NBMA mode could be used in an ATM, Frame Relay, SMDS, PRI ISDN, or X.25 network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number*
4. **ip pim nbma-mode**
5. **ip pim multipoint-signalling**
6. **atm multipoint-signalling**
7. **ip pim vc-count** *number*
8. **ip pim minimum-vc-rate** *pps*
9. **show ip pim vc**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *number* **Example:** `Router(config)# interface atm 0`	Configures an ATM interface.
Step 4	**ip pim nbma-mode** **Example:** `Router(config-if)# ip pim nbma-mode`	(Optional) Enables NBMA mode on a serial link.

	Command or Action	Purpose
Step 5	**ip pim multipoint-signalling** **Example:** `Router(config-if)# ip pim multipoint-signalling`	Enables IP multicast over ATM point-to-multipoint VCs. • This command enables PIM to open ATM point-to-multipoint VCs for each multicast group that a receiver joins.
Step 6	**atm multipoint-signalling** **Example:** `Router(config-if)# atm multipoint-signalling`	Enables point-to-multipoint signaling to the ATM switch. • This command is required so that static map multipoint VCs can be opened. The router uses existing static map entries that include the **broadcast** keyword to establish multipoint calls. The map list is needed because it acts like a static ARP table.
Step 7	**ip pim vc-count** *number* **Example:** `Router(config-if)# ip pim vc-count 300`	(Optional) Changes the maximum number of VCs that PIM can open. • By default, PIM can open a maximum of 200 VCs. When the router reaches this number, it deletes inactive VCs so it can open VCs for new groups that might have activity.
Step 8	**ip pim minimum-vc-rate** *pps* **Example:** `Router(config-if)# ip pim minimum-vc-rate 1500`	(Optional) Sets the minimum activity rate required to keep VCs from being idled. • By default, all VCs are eligible for idling.
Step 9	**show ip pim vc** **Example:** `Router# show ip pim vc`	(Optional) Displays ATM VC status information for multipoint VCs opened by PIM.

Configuration Examples for IP Multicast over ATM Point-to-Multipoint VCs

IP Multicast over ATM Point-to-Multipoint VCs Example

The following example shows how to enable IP multicast over ATM point-to-multipoint VCs:

```
interface ATM2/0
ip address 171.69.214.43 255.255.255.248
```

```
 ip pim sparse-mode
 ip pim multipoint-signalling
 ip ospf network broadcast
 atm nsap-address 47.00918100000000410B0A1981.333333333333.00
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 atm multipoint-signalling
 map-group mpvc
router ospf 9
 network 171.69.214.0 0.0.0.255 area 0
!
ip classless
 ip pim rp-address 171.69.10.13 98
!
map-list mpvc
 ip 171.69.214.41 atm-nsap 47.00918100000000410B0A1981.111111111111.00 broadcast
 ip 171.69.214.42 atm-nsap 47.00918100000000410B0A1981.222222222222.00 broadcast
 ip 171.69.214.43 atm-nsap 47.00918100000000410B0A1981.333333333333.00 broadcast
```

Additional References

Related Documents

Related Topic	Document Title
IP multicast commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Multicast Command Reference, Release 12.4*

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Feature Information for Configuring IP Multicast over ATM Point-to-Multipoint VCs

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for IP Multicast over ATM Point-to-Multipoint VCs

Feature Name	Releases	Feature Configuration Information
This table is intentionally left blank because no features were introduced or modified in Cisco IOS Release 12.2(1) or later. This table will be updated when feature information is added to this module.	--	--

Configuring PGM Host and Router Assist

Note Support for the PGM Host feature has been removed. Use of this feature is not recommended.

This module describes the PGM Host and Router Assist feature. PGM Host and Router Assist enables Cisco routers to support multicast applications that operate at the PGM transport layer and the PGM network layer, respectively.

The PGM Reliable Transport Protocol itself is implemented on the hosts of the customer. For information on PGM Reliable Transport Protocol, refer to the Internet Engineering Task Force (IETF) protocol specification draft named *PGM Reliable Transport Protocol Specification* .

Information About PGM Host and Router Assist

PGM Overview

Note Support for the PGM Host feature has been removed. Use of this feature is not recommended.

Pragmatic General Multicast (PGM) is a reliable multicast transport protocol for multicast applications that require reliable, ordered, duplicate-free multicast data delivery from multiple sources to multiple receivers. PGM guarantees that a receiver in a multicast group either receives all data packets from transmissions and retransmissions, or can detect unrecoverable data packet loss. PGM is intended as a solution for multicast applications with basic reliability requirements. PGM has two main parts: a host element (also referred to as the transport layer of the PGM protocol) and a network element (also referred to as the network layer of the PGM protocol).

The transport layer of the PGM protocol has two main parts: a source part and a receiver part. The transport layer defines how multicast applications send and receive reliable, ordered, duplicate-free multicast data from multiple sources to multiple receivers. PGM Host is the Cisco implementation of the transport layer of the PGM protocol.

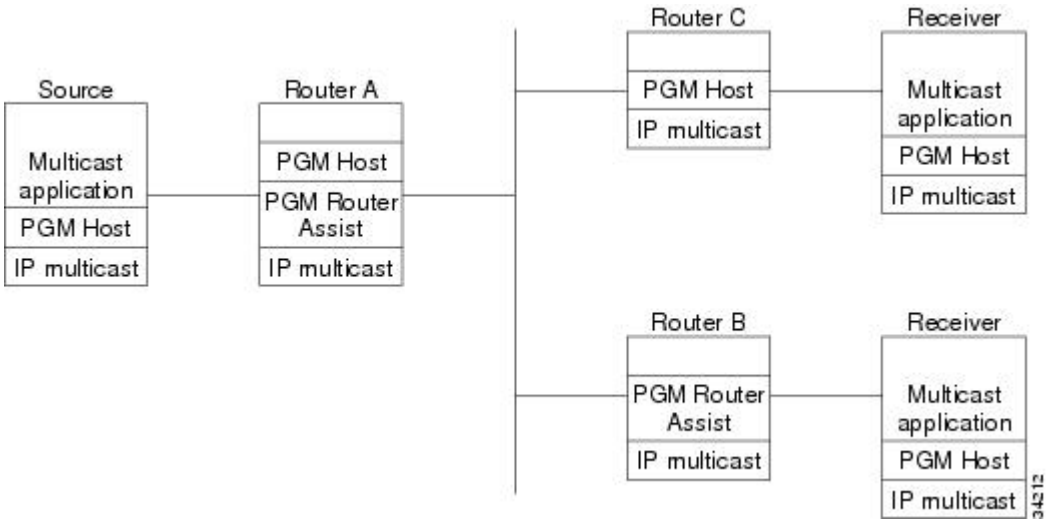
The network layer of the PGM protocol defines how intermediate network devices (such as routers and switches) handle PGM transport data as the data flows through a network. PGM Router Assist is the Cisco implementation of the network layer of the PGM protocol.

Note PGM contains an element that assists routers and switches in handling PGM transport data as it flows through a network. Unlike the Router Assist element, the Host element does not have a current practical application.

PGM is network-layer independent; PGM Host and Router Assist in the Cisco IOS software support PGM over IP. Both PGM Host and Router Assist use a unique transport session identifier (TSI) that identifies each individual PGM session.

The figure shows a simple network topology using the PGM Host and Router Assist feature.

Figure 2



When the router is functioning as a network element (PGM Router Assist is configured) and PGM Host is configured (Router A in the figure), the router can process received PGM packets as a virtual PGM Host, originate PGM packets and serve as its own first hop PGM network element, and forward received PGM packets.

When the router is functioning as a network element and PGM Host is not configured (Router B in the figure), the router forwards received PGM packets as specified by PGM Router Assist parameters.

When the router is not functioning as a network element and PGM Host is configured (Router C in the figure), the router can receive and forward PGM packets on any router interface simultaneously as specified by PGM Host feature parameters. Although this configuration is supported, it is not recommended in a PGM network because PGM Host works optimally on routers that have PGM Router Assist configured.

How to Configure PGM Host and Router Assist

Note Support for the PGM Host feature has been removed. Use of this feature is not recommended.

Enabling PGM Host

Note Support for the PGM Host feature has been removed. Use of this feature is not recommended.

When enabling PGM Host on your router, you must source PGM packets through a vif or out a physical interface installed in the router.

Sourcing PGM packets through a vif enables the router to send and receive PGM packets through any router interface. The vif also serves as the interface to the multicast applications that reside at the PGM network layer.

Sourcing IP multicast traffic out a specific physical or logical interface type (for example, an Ethernet, serial, or loopback interface) configures the router to send PGM packets out that interface only and to receive packets on any router interface.

Prerequisites

- PGM Reliable Transport Protocol is configured on hosts connected to your network.
- PGM Router Assist is configured on intermediate routers and switches connected to your network.
- IP multicast routing is configured on all devices connected to your network that will be processing IP multicast traffic, including the router on which you are configuring PGM Host.
- Protocol Independent Multicast (PIM) or another IP multicast routing protocol is configured on each PGM interface in your network that will send and receive IP multicast packets.
- A PGM multicast virtual host interface (vif) is configured on the router (if you do not plan to source PGM packets through a physical interface installed on the router). The vif enables the router to send and receive IP multicast packets on several different interfaces at once, as dictated by the multicast routing tables on the router.

Enabling PGM Host with a Virtual Host Interface

To enable PGM Host globally on the router and to configure the router to source PGM packets through a vif, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ip pgm host`	Enables PGM Host (both the source and receiver parts of the PGM network layer) globally on the router and configures the router to source PGM packets through a vif. **Note** You must configure a vif by using the **interface vif** *number* global configuration command on the router before enabling PGM Host on the router; otherwise, the router will not know to use the vif to source PGM packets and PGM Host will not be enabled on the router.

See the PGM Host with a Virtual Interface Example, page 16 section later in this module for an example of enabling PGM Host with a virtual interface.

Enabling PGM Host with a Physical Interface

To enable PGM Host globally on the router and to configure the router to source PGM packets through a physical interface, use the following commands in global configuration mode:

SUMMARY STEPS

1. Router(config)# **ip pgm host**
2. Router(config)# **ip pgm host source-interface** *type number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **ip pgm host**	Enables PGM Host (both the source and receiver part of the PGM network layer) globally on the router.
Step 2	Router(config)# **ip pgm host source-interface** *type number*	Configures the router to source PGM packets through a physical (or logical) interface.

See the PGM Host with a Physical Interface Example, page 17 section later in this module for an example of enabling PGM Host with a physical interface.

Verifying PGM Host Configuration

Note Support for the PGM Host feature has been removed. Use of this feature is not recommended.

To verify that PGM Host is configured correctly on your router, use the following **show** commands in EXEC mode:

- Use the **show ip pgm host sessions** command to display information about current open PGM transport sessions:

```
Router> show ip pgm host sessions
```

```
Idx  GSI           Source Port  Type     State   Dest Port  Mcast Address
1    000000000000  0            receiver listen  48059      224.3.3.3
2    9CD72EF099FA  1025         source   conn    48059      224.1.1.1
```

Specifying a traffic session number or a multicast IP address with the **show ip pgm host sessions**command displays information specific to that PGM transport session:

```
Router> show ip pgm host sessions 2
Idx  GSI           Source Port  Type     State   Dest Port  Mcast Address
2    9CD72EF099FA  1025         source   conn    48059      224.1.1.1

    stream-type (apdu), ttl (255)

    spm-ambient-ivl (6000), txw-adv-secs (6000)
    txw-adv-timeout-max (3600000), txw-rte (16384), txw-secs (30000)
    ncf-max (infinite), spm-rpt-ivl (3000), ihb-min (1000)
    ihb-max (10000), join (0), tpdu-size (16384)
    txw-adv-method (time), tx-buffer-mgmt (return)

    ODATA packets sent                      0
          bytes sent                        0
    RDATA packets sent                      0
          bytes sent                        0
    Total bytes sent                        0
    ADPUs sent                              0
    APDU  transmit memory errors            0
    SPM   packets sent                      6
    NCF   packets sent                      0
    NAK   packets received                  0
          packets received in error         0
    General bad packets                     0
    TX window lead                          0
    TX window trail                         0
```

- Use the **show ip pgm host traffic**command to display traffic statistics at the PGM transport layer:

```
Router> show ip pgm host traffic
General Statistics :

    Sessions in                             0
             out                            0
    Bytes    in                             0
             out                            0

Source Statistics :

    ODATA packets sent                      0
          bytes sent                        0
    RDATA packets sent                      0
          bytes sent                        0
    Total bytes sent                        0
    ADPUs sent                              0
    APDU  transmit memory errors            0
    SPM   packets sent                      0
    NCF   packets sent                      0
    NAK   packets received                  0
          packets received in error         0

Receiver Statistics :

    ODATA packets received                  0
          packets received in error         0
          valid bytes received              0
    RDATA packets received                  0
          packets received in error         0
          valid bytes received              0
    Total valid bytes received              0
    Total bytes received in error           0
    ADPUs received                          0
    SPM   packets received                  0
          packets received in error         0
    NCF   packets received                  0
```

```
      packets received in error          0
NAK   packets received                   0
      packets received in error          0
      packets sent                       0
Undeliverable packets                    0
General bad packets                      0
Bad checksum packets                     0
```

Enabling PGM Router Assist

When enabling PGM Router Assist on your router, you must set up your router to forward PGM packets through a vif or out a physical interface installed in the router.

Setting up your router to forward PGM packets through a vif enables the router to forward PGM packets through any router interface. The vif also serves as the interface to the multicast applications that reside at the PGM network layer.

Setting up your router to forward PGM packets out a specific physical or logical interface type (for example, an Ethernet, serial, or loopback interface) configures the router to forward PGM packets out that interface only.

Prerequisites

- PGM Reliable Transport Protocol is configured on hosts connected to your network.
- IP multicast is configured on the router upon which you will enable PGM Router Assist.
- PIM is configured on each PGM interface.

Enabling PGM Router Assist with a Virtual Host Interface

To enable PGM Router Assist on a vif, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **ip pgm router**	Enables the router to assist PGM on this interface. **Note** You must configure a vif by using the **interface vif** *number* global configuration command on the router before enabling PGM Assist on the router; otherwise, PGM Assist will not be enabled on the router.

Enabling PGM Router Assist with a Physical Interface

To enable PGM Router Assist on the router and to configure the router to forward PGM packets through a physical interface, use the following commands in interface configuration mode:

Command	Purpose
`Router(config-if)# ip pgm router`	Enables the router to assist PGM on this interface.

Monitoring and Maintaining PGM Host and Router Assist

This section provides information on monitoring and maintaining the PGM Host and Router Assist feature.

Monitoring and Maintaining PGM Host

Note Support for the PGM Host feature has been removed. Use of this feature is not recommended.

To reset PGM Host connections, use the following command in privileged EXEC mode:

Command	Purpose
`Router# clear ip pgm host defaults traffic }`	Resets PGM Host connections to their default values and clears traffic statistics.

To enable PGM Host debugging, use the following command in privileged EXEC mode:

Command	Purpose
`Router# debug ip pgm host`	Displays debug messages for PGM Host.

To display PGM Host information, use the following commands in user EXEC mode, as needed:

Command	Purpose
`Router> show ip pgm host defaults`	Displays the default values for PGM Host traffic.
`Router> show ip pgm host sessions [ session-number group-address ]`	Displays open PGM Host traffic sessions.
`Router> show ip pgm host traffic`	Displays PGM Host traffic statistics.

Monitoring and Maintaining PGM Router Assist

To clear PGM traffic statistics, use the following command in privileged EXEC mode:

Command	Purpose
`Router#` **clear ip pgm router** [[**traffic** [*type number*]] | [**rtx-state** [*group-address*]]]	Clears the PGM traffic statistics. Use the **rtx-state** keyword to clear PGM retransmit state.

To display PGM information, use the following command in privileged EXEC mode:

Command	Purpose
`Router#` **show ip pgm router** [[**interface** [*type number*]] | [**state** [*group-address*]] | [**traffic** [*type number*]]] [**verbose**]	Displays information about PGM traffic statistics and TSI state. The TSI is the transport-layer identifier for the source of a PGM session. Confirms that PGM Router Assist is configured, although there might not be any active traffic. Use the **state** or **traffic** keywords to learn whether an interface is actively using PGM.

PGM Host and Router Assist Configuration Examples

Note Support for the PGM Host feature has been removed. Use of this feature is not recommended.

PGM Host with a Virtual Interface Example

Note Support for the PGM Host feature has been removed. Use of this feature is not recommended.

The following example shows PGM Host (both the source and receiver part of the PGM network layer) enabled globally on the router and PGM packets sourced through virtual host interface 1 (vif1). PGM packets can be sent and received on the vif and on the two physical interfaces (ethernet1 and ethernet2) simultaneously.

```
ip multicast-routing
ip routing
ip pgm host
interface vif1
ip address 10.0.0.1 255.255.255.0
ip pim dense-mode
no ip directed-broadcast
no ip mroute-cache
interface ethernet1
ip address 10.1.0.1 255.255.255.0
ip pim dense-mode
no ip directed-broadcast
no ip mroute-cache
```

```
media-type 10BaseT
interface ethernet2
ip address 10.2.0.1 255.255.255.0
ip pim dense-mode
no ip directed-broadcast
no ip mroute-cache
media-type 10BaseT
```

PGM Host with a Physical Interface Example

Note Support for the PGM Host feature has been removed. Use of this feature is not recommended.

The following example shows PGM Host (both the source and receiver part of the PGM network layer) enabled globally on the router and PGM packets sourced out of physical Ethernet interface 1. PGM packets can be received on physical Ethernet interfaces 1 and 2 simultaneously.

```
ip multicast-routing
ip routing
ip pgm host
ip pgm host source-interface ethernet1
ip pgm host source-interface ethernet2
interface ethernet1
ip address 10.1.0.1 255.255.255.0
ip pim dense-mode
no ip directed-broadcast
no ip mroute-cache
media-type 10BaseT
interface ethernet2
ip address 10.2.0.1 255.255.255.0
ip pim dense-mode
no ip directed-broadcast
no ip mroute-cache
media-type 10BaseT
```

PGM Router Assist with a Virtual Interface Example

The following example shows PGM Router Assist (the PGM network layer) enabled on the router and the router set up to forward PGM packets on virtual host interface 1 (vif1). PGM packets can be received on interfaces vif1, ethernet1, and ethernet2 simultaneously.

```
ip multicast-routing
ip routing
interface vif1
ip address 10.0.0.1 255.255.255.0
ip pim dense-mode
ip pgm router
no ip directed-broadcast
no ip mroute-cache
interface ethernet1
ip address 10.1.0.1 255.255.255.0
ip pim dense-mode
ip pgm router
no ip directed-broadcast
no ip mroute-cache
media-type 10BaseT
interface ethernet2
ip address 10.2.0.1 255.255.255.0
ip pim dense-mode
ip pgm router
no ip directed-broadcast
no ip mroute-cache
```

media-type 10BaseT

PGM Router Assist with a Physical Interface Example

The following example shows PGM Router Assist (the PGM network layer) enabled on the router and the router set up to forward PGM packets out of physical Ethernet interfaces 1 and 2. PGM packets can be received on physical Ethernet interfaces 1 and 2 simultaneously.

```
ip multicast-routing
ip routing
interface ethernet1
ip address 10.1.0.1 255.255.255.0
ip pim dense-mode
ip pgm router
no ip directed-broadcast
no ip mroute-cache
media-type 10BaseT
interface ethernet2
ip address 10.2.0.1 255.255.255.0
ip pim dense-mode
ip pgm router
no ip directed-broadcast
no ip mroute-cache
media-type 10BaseT
```

Feature Information for PGM Host and Router Assist

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2 Feature Information for PGM Host and Router Assist

Feature Name	Releases	Feature Information
Pragmatic General Multicast (PGM)	12.2(15)T	Pragmatic General Multicast (PGM) is a reliable multicast transport pro-tocol for applications that require ordered, duplicate-free, multicast data delivery from multiple sources to multiple receivers.
PGM Host	12.2(15)T	PGM has two primary parts; network element and host style functions. This feature implements the host side functionality of PGM.

Using the Multicast Routing Monitor

The Multicast Routing Monitor (MRM) is a management diagnostic tool that provides network fault detection and isolation in a large multicast routing infrastructure. It is designed to notify a network administrator of multicast routing problems in a test environment.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Using the Multicast Routing Monitor

You must make sure the underlying multicast forwarding network being tested has no access lists or boundaries that deny the MRM data and control traffic. Specifically, consider the following factors:

- MRM test data are User Datagram Protocol (UDP) and Real-Time Transport Protocol (RTP) packets addressed to the configured multicast group address.
- MRM control traffic between the Test Sender, Test Receiver, and Manager is addressed to the 224.0.1.111 multicast group, which all three components join. The 224.0.1.111 group is an IANA-registered group.
- Take into account the unicast IP addresses of sources and receivers when considering what could prevent control traffic flowing.

Information About the Multicast Routing Monitor

Multicast Routing Monitor Operation

MRM has three components that play different roles: the Manager, the Test Sender, and the Test Receiver. To test a multicast environment using test packets, perhaps before an upcoming multicast event, you need all three components.

You create a test based on various test parameters, name the test, and start the test. The test runs in the background and the command prompt returns.

If the Test Receiver detects an error (such as packet loss or duplicate packets), it sends an error report to the router configured as the Manager. The Manager immediately displays the error report. (The **show ip mrm status-report**command also displays error reports, if any.) You then troubleshoot your multicast environment as normal, perhaps using the **mtrace** command from the source to the Test Receiver. If the **show ip mrm status-report**command displays no error reports, the Test Receiver is receiving test packets without loss or duplicates from the Test Sender.

The Cisco implementation of MRM supports Internet Draft of Multicast Routing Monitor (MRM), Internet Engineering Task Force (IETF), March 1999. The IETF originally conceived MRM to use both test packets and real data. The Cisco implementation does not use real data due to technical issues and the fact that the IETF draft did not progress.

Benefits of Multicast Routing Monitor

The benefits of the MRM are as follows:

- MRM allows network personnel to generate test flows without having to use host devices.
- MRM can verify a multicast environment prior to an event. You need not wait for real multicast traffic to fail in order to find out that a problem exists. You can test the multicast routing environment before a planned event.
- MRM provides easy diagnostics. The error information is easy for the user to understand.
- MRM is scalable. This diagnostic tool works well for many users.

How to Use the Multicast Routing Monitor

Configuring a Test Receiver

Perform this task to configure a Test Receiver on a router or host.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip mrm test-receiver**
5. **exit**
6. **ip mrm accept-manager** *access-list*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/0`	Specifies an interface, and enters interface configuration mode.
Step 4	**ip mrm test-receiver** **Example:** `Router(config-if)# ip mrm test-receiver`	Configures the interface to operate as a Test Receiver.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Returns to the next higher configuration mode.

	Command or Action	Purpose
Step 6	**ip mrm accept-manager** *access-list* **Example:** `Router(config)# ip mrm accept-manager supervisor`	(Optional) Specifies that the Test Receiver can accept status report requests only from Managers specified by the access list. • The access list is required and can be named or numbered. • This example uses an access list named “supervisor.” The access list is presumed to be already configured.

Configuring a Test Sender

Perform this task to configure a Test Sender on a different router or host from where you configured the Test Receiver.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip mrm test-sender**
5. **exit**
6. **ip mrm accept-manager** [*access-list*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigiabitethernet 0/0/0`	Specifies an interface, and enters interface configuration mode.

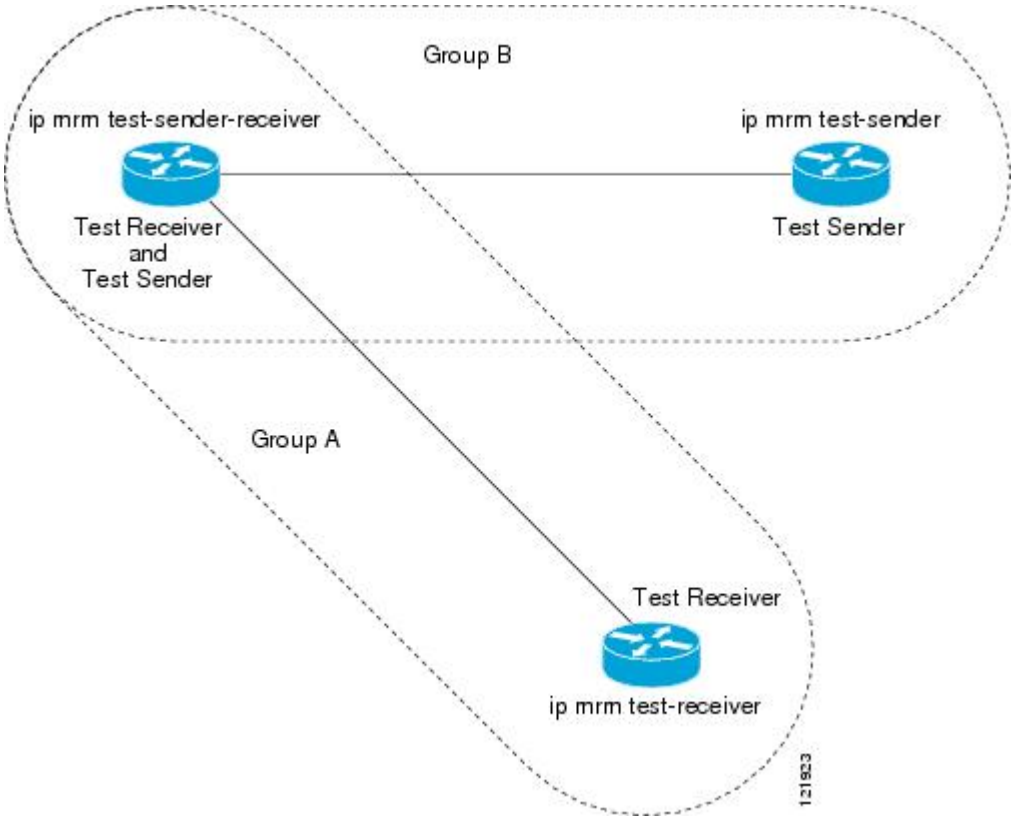
	Command or Action	Purpose
Step 4	**ip mrm test-sender** **Example:** `Router(config-if)# ip mrm test-sender`	Configures the interface to operate as a Test Sender.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Returns to the next higher configuration mode.
Step 6	**ip mrm accept-manager** [*access-list*] **Example:** `Router(config)# ip mrm accept-manager supervisor`	(Optional) Specifies that the Test Sender can accept status report requests only from Managers specified by the access list. • This example uses an access list named “supervisor.” The access list is presumed to be already configured.

Monitoring Multiple Groups

If you have more than one multicast group to monitor, you can configure an interface that is a Test Sender for one group and a Test Receiver for another group.

The figure illustrates an environment where the router on the left is the Test Sender for Group A and the Test Receiver for Group B.

Figure 3



SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip mrm test-sender-receiver**
5. **exit**
6. **ip mrm accept-manager** *access-list* [**test-sender** | **test-receiver**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/0`	Specifies an interface, and enters interface configuration mode.
Step 4	**ip mrm test-sender-receiver** **Example:** `Router(config-if)# ip mrm test-sender-receiver`	Configures the interface to operate as a Test Sender for one group and Test Receiver for another group.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Returns to the next higher configuration mode.
Step 6	**ip mrm accept-manager** *access-list* [**test-sender** | **test-receiver**] **Example:** `Router(config)# ip mrm accept-manager supervisor test-sender`	(Optional) Specifies that the Test Sender or Test Receiver can accept status report requests only from Managers specified by the access list. • By default, the command applies to both the Test Sender and Test Receiver. Because this device is both, you might need to specify that the restriction applies to only the Test Sender or only the Test Receiver using the **test-sender** keyword or **test-receiver** keyword, respectively.

Configuring a Manager

Perform this task to configure a router as a Manager in order for MRM to function.

Note A host cannot be a Manager.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip mrm manager** *test-name*
4. **manager** *type number* **group** *ip-address*
5. **beacon** [**interval** *seconds*] [**holdtime** *seconds*][**ttl** *ttl-value*]
6. **udp-port test-packet** *port-number*] **status-report** *port-number* **]**
7. **senders** access-list [**packet-delay** *milliseconds*] [**rtp**| **udp**] [**target-only**| **all-multicasts**| **all-test-senders**]
8. **receivers** *access-list* **sender-list** *access-list* [*packet-delay*]
9. **receivers** *access-list* [**window** *seconds*] [**report-delay** *seconds*] [**loss** *percentage*] [**no-join**] [**monitor** | **poll**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip mrm manager** *test-name* **Example:** `Router(config)# ip mrm manager test1`	Specifies the name of an MRM test to be created or modified, and enters MRM manager configuration mode. • The test name is used to start, stop, and monitor a test. • From MRM manager configuration mode, you specify the parameters of the test.
Step 4	**manager** *type number* **group** *ip-address* **Example:** `Router(config-mrm-manager)# manager gigabitethernet 0/0/0 group 239.1.1.1`	Specifies which interface on the router is the Manager, and specifies the multicast group address the Test Receiver will listen to.

	Command or Action	Purpose
Step 5	**beacon** [**interval** *seconds*] [**holdtime** *seconds*][**ttl** *ttl-value*] **Example:** `Router(config-mrm-manager)# beacon interval 60`	(Optional) Changes the frequency, duration, or scope of beacon messages that the Manager sends to the Test Sender and Test Receiver. • By default, beacon messages are sent at an interval of 60 seconds. • By default, the duration of a test period is 86400 seconds (1 day). • By default, the TTL is 32 hops.
Step 6	**udp-port test-packet** *port-number*] **status-report** *port-number* **]** **Example:** `Router(config-mrm-manager)# udp-port test-packet 20202`	(Optional) Changes the UDP port numbers to which the Test Sender sends test packets or the Test Receiver sends status reports. • Use the optional **test-packet** keyword and *port-number* argument to change the UDP port to which the Test Sender sends test packets. The port number must be even if the packets are Real-Time Transport Protocol (RTP)-encapsulated. The range is from 16384 to 65535. • By default, the Test Sender uses UDP port number 16834 to send test packets. • Use the optional **status-report** keyword and *port-number* argument to change the UDP port to which the Test Receiver sends status reports. The port number must be odd if the packets are RTP Control Protocol (RTCP)-encapsulated. The range is from 16834 to 65535. • By default, the Test Receiver uses UDP port number 65535 to send status reports.
Step 7	**senders** access-list [**packet-delay** *milliseconds*] [**rtp**| **udp**] [**target-only**| **all-multicasts**| **all-test-senders**] **Example:** `Router(config-mrm-manager)# senders 1 packet-delay 400 udp all-test-senders`	Establishes Test Senders for MRM tests. • Use the optional **packet-delay** keyword and *milliseconds* argument to specify the delay between test packets (in milliseconds). The range is from 50 to 10000. The default is 200 milliseconds, which results in 5 packets per second. • Use the optional **rtp** keyword or **udp** keyword to specify the encapsulation of test packets, either Real-Time Transport Protocol (RTP) encapsulated or User Datagram Protocol (UDP) encapsulated. By default, test packets are RTP-encapsulated. • Use the optional **target-only** keyword to specify that test packets are sent out on the targeted interface only (that is, the interface with the IP address that is specified in the Test Sender request target field). By default, test packets are sent out on all interfaces that are enabled with IP multicast. • Use the optional **all-multicasts** keyword to specify that the test packets are sent out on all interfaces that are enabled with IP multicast. This is the default method for sending test packets. • Use the optional **all-test-senders** keyword to specify that test packets are sent out on all interfaces that have test-sender mode enabled. By default, test packets are sent out on all interfaces that are enabled with IP multicast.

	Command or Action	Purpose
Step 8	**receivers** *access-list* **sender-list** *access-list* [*packet-delay*] **Example:** `Router(config-mrm-manager)# receivers 1 sender-list 3`	Establishes Test Receivers for MRM. **Note** Although the Cisco IOS CLI parser accepts the command entered without the **sender-list** *access-list* keyword-argument pair, this keyword-argument pair is not optional. For an MRM test to work, you must specify the sources that the Test Receiver should monitor using the **sender-list** keyword and *access-list* argument. • Use the **sender-list** keyword and *access-list* to specify the sources that the Test Receiver should monitor. If the named or numbered access list matches any access list specified in the **senders** command, the associated **packet-delay** *milliseconds* keyword and argument of that **senders** command are used in the MRM test. Otherwise, the **receivers** command requires that a delay be specified for the *packet-delay* argument. • Use the optional *packet-delay* argument to specify the delay between test packets (in milliseconds). The range is from 50 to 10000. If the **sender-list** access list matches any access list specified in a **senders** command, the associated **packet-delay** *milliseconds* keyword and argument of that **senders** command are used in this command. Otherwise, the **receivers**command requires that a delay be specified for the *packet-delay* argument.
Step 9	**receivers** *access-list* [**window** *seconds*] [**report-delay** *seconds*] [**loss** *percentage*] [**no-join**] [**monitor** | **poll**] **Example:** `Router(config-mrm-manager)# receivers 1 window 7 report-delay 30`	(Optional) Modifies the parameters of Test Receivers. • Use the optional **window** keyword and *seconds* argument to specify the duration (in seconds) of a test period. This is a sliding window of time in which the packet count is collected, so that the loss percentage can be calculated. The range is from 1 to 10. The default is 5 seconds. • Use the optional **report-delay** keyword and *seconds* argument to specify the delay (in seconds) between status reports. The delay prevents multiple Test Receivers from sending status reports to the Manager at the same time for the same failure. This value is relevant only if there are multiple Test Receivers. The range is from 1 to 60. The default is 1 second. • Use the optional **loss** keyword and *percentage* argument to specify the threshold percentage of packet loss required before a status report is triggered. The range is from 0 to 100. The default is 0 percent, which means that a status report is sent for any packet loss. • Use the optional **no-join** keyword to specify that the Test Receiver does not join the monitored group. The default is that the Test Receiver joins the monitored group. • Use either the optional **monitor** or **poll** keyword to specify whether the Test Receiver monitors the test group or polls for receiver statistics. The **monitor** keyword means the Test Receiver reports only if the test criteria are met. The **poll** keyword means the Test Receiver sends status reports regularly, whether test criteria are met or not. The default is the behavior set with the **monitor** keyword.

Conducting an MRM Test and Viewing Results

From the router playing the Manager role you can start and stop the MRM test. To start and subsequently stop your MRM test, perform this task.

When the test begins, the Manager sends a unicast control packet to the Test Sender and Test Receiver, and then the Manager starts sending beacons. The Test Sender and Test Receiver send acknowledgments to the Manager and begin sending or receiving test packets. If an error occurs, the Test Receiver sends an error report to the Manager, which immediately displays the report.

SUMMARY STEPS

1. **enable**
2. **clear ip mrm status-report** [*ip-address*]
3. **show ip mrm interface** [*type number*]
4. **show ip mrm manager** [*test-name*]
5. **mrm** *test-name* **start**
6. **mrm** *test-name* **stop**
7. **show ip mrm status-report** [*ip-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ip mrm status-report** [*ip-address*] **Example:** `Router# clear ip mrm status-report 172.16.0.0`	(Optional) Clears the MRM status report cache.
Step 3	**show ip mrm interface** [*type number*] **Example:** `Router# show ip mrm interface Ethernet 1`	(Optional) Displays MRM information related to interfaces. • Use this command before starting an MRM test to verify the interfaces are participating in MRM, in which roles, and whether the interfaces are up or down.
Step 4	**show ip mrm manager** [*test-name*] **Example:** `Router# show ip mrm manager test1`	(Optional) Displays information about MRM tests. • Use this command before starting an MRM test to verify MRM status information and the parameters configured for an MRM test.

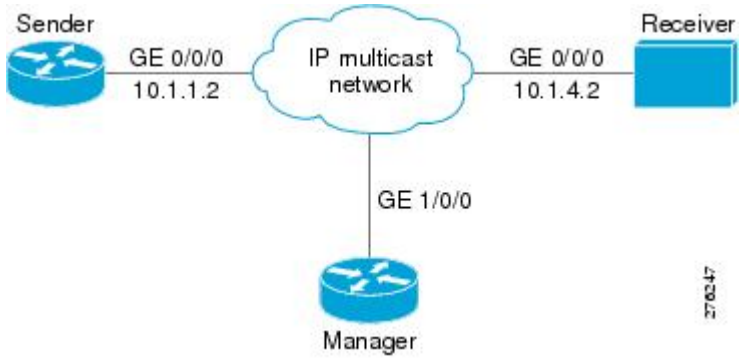
	Command or Action	Purpose
Step 5	**mrm** *test-name* **start** **Example:** `Router# mrm test1 start`	Starts the MRM test.
Step 6	**mrm** *test-name* **stop** **Example:** `Router# mrm test1 stop`	Stops the MRM test.
Step 7	**show ip mrm status-report** [*ip-address*] **Example:** `Router# show ip mrm status-report`	(Optional) Displays the status reports in the MRM status report cache.

Configuration Examples for MRM

Configuring MRM Example

The figure illustrates a Test Sender, a Test Receiver, and a Manager in an MRM environment. The partial configurations for the three devices follow the figure.

Figure 4



Test Sender Configuration

```
interface GigabitEthernet 0/0/0
 ip mrm test-sender
```

Test Receiver Configuration

```
interface GigabitEthernet 0/0/0
 ip mrm test-receiver
```

Manager Configuration

```
ip mrm manager test1
manager GigabitEthernet 1/0/0 group 239.1.1.1
senders 1
receivers 2 sender-list 1
!
access-list 1 permit 10.1.1.2
access-list 2 permit 10.1.4.2
```

Additional References

Related Documents

Related Topic	Document Title
IP multicast commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Multicast Command Reference*

Standards

Standard	Title
draft-ietf-mboned-mrm-use-00.txt	Justification and Use of the Multicast Routing Monitor (MRM) Protocol

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Using the Multicast Routing Monitor

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3 Feature Information for Using the Multicast Routing Monitor

Feature Name	Releases	Feature Information
Multicast Routing Monitor (MRM)	12.2(15)T	The Multicast Routing Monitor is a network fault detection and isolation mechanism for administering a multicast routing infrastructure.

trademarks mentioned 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. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Configuring DVMRP Interoperability

Note Distance Vector Multicast Routing Protocol (DVMRP) CLI and functionality are not provided in Cisco IOS software images that provide MTR support.

This module describes the DVMRP Interoperability feature. Cisco routers run Protocol Independent Multicast (PIM), and know enough about DVMRP to successfully forward multicast packets to and receive packets from a DVMRP neighbor. It is also possible to propagate DVMRP routes into and through a PIM cloud. The Cisco IOS software propagates DVMRP routes and builds a separate database for these routes on each router, but PIM uses this routing information to make the packet-forwarding decision. Cisco IOS software does not implement the complete DVMRP.

DVMRP builds a parent-child database using a constrained multicast model to build a forwarding tree rooted at the source of the multicast packets. Multicast packets are initially flooded down this source tree. If redundant paths are on the source tree, packets are not forwarded along those paths. Forwarding occurs until prune messages are received on those parent-child links, which further constrains the broadcast of multicast packets.

DVMRP is implemented in the equipment of many vendors and is based on the public-domain mrouted program. The Cisco IOS software supports dynamic discovery of DVMRP routers and can interoperate with them over traditional media such as Ethernet and FDDI, or over DVMRP-specific tunnels.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release.

Basic DVMRP Interoperability Configuration Task List

To configure basic interoperability with DVMRP machines, perform the tasks described in the following sections. The tasks in the first section are required; the tasks in the remaining sections are optional.

For more advanced DVMRP interoperability features, see the section "Advanced DVMRP Interoperability Configuration Task List, page 41" later in this chapter.

Configuring DVMRP Interoperability

Cisco multicast routers using PIM can interoperate with non-Cisco multicast routers that use the DVMRP.

PIM routers dynamically discover DVMRP multicast routers on attached networks. Once a DVMRP neighbor has been discovered, the router periodically sends DVMRP report messages advertising the unicast sources reachable in the PIM domain. By default, directly connected subnets and networks are advertised. The router forwards multicast packets that have been forwarded by DVMRP routers and, in turn, forwards multicast packets to DVMRP routers.

You can configure which sources are advertised and which metrics are used by configuring the **ip dvmrp metric** interface configuration command. You can also direct all sources learned via a particular unicast routing process to be advertised into DVMRP.

The mrouted protocol is a public-domain implementation of DVMRP. It is necessary to use mrouted Version 3.8 (which implements a nonpruning version of DVMRP) when Cisco routers are directly connected to DVMRP routers or interoperate with DVMRP routers over an multicast backbone (MBONE) tunnel. DVMRP advertisements produced by the Cisco IOS software can cause older versions of mrouted to corrupt their routing tables and those of their neighbors. Any router connected to the MBONE should have an access list to limit the number of unicast routes that are advertised via DVMRP.

To configure the sources that are advertised and the metrics that are used when DVMRP report messages are sent, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **ip dvmrp metric** *metric* [**list** *access-list*] [*protocol process-id*]	Configures the metric associated with a set of destinations for DVMRP reports.

A more sophisticated way to achieve the same results as the preceding command is to use a route map instead of an access list. Thus, you have a finer granularity of control. To subject unicast routes to route map conditions before they are injected into DVMRP, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **ip dvmrp metric** *metric* [**route-map** *map-name*]	Subjects unicast routes to route map conditions before they are injected into DVMRP.

Responding to mrinfo Requests

The Cisco IOS software answers mrinfo requests sent by mrouted systems and Cisco routers. The software returns information about neighbors on DVMRP tunnels and all of the interfaces of the router. This information includes the metric (which is always set to 1), the configured TTL threshold, the status of the

interface, and various flags. The **mrinfo** EXEC command can also be used to query the router itself, as in the following example:

```
mm1-7kd# mrinfo
  171.69.214.27 (mm1-7kd.cisco.com) [version cisco 11.1] [flags: PMS]:
  171.69.214.27 -> 171.69.214.26 (mm1-r7kb.cisco.com) [1/0/pim/querier]
  171.69.214.27 -> 171.69.214.25 (mm1-45a.cisco.com) [1/0/pim/querier]
  171.69.214.33 -> 171.69.214.34 (mm1-45c.cisco.com) [1/0/pim]
  171.69.214.137 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
  171.69.214.203 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
  171.69.214.18 -> 171.69.214.20 (mm1-45e.cisco.com) [1/0/pim]
  171.69.214.18 -> 171.69.214.19 (mm1-45c.cisco.com) [1/0/pim]
  171.69.214.18 -> 171.69.214.17 (mm1-45a.cisco.com) [1/0/pim]
```

See the "DVMRP Interoperability Example, page 46" section later in this chapter for an example of how to configure a PIM router to interoperate with a DVMRP router.

Configuring a DVMRP Tunnel

The Cisco IOS software supports DVMRP tunnels to the MBONE. You can configure a DVMRP tunnel on a router if the other end is running DVMRP. The software then sends and receives multicast packets over the tunnel. This strategy allows a PIM domain to connect to the DVMRP router in the case where all routers on the path do not support multicast routing. You cannot configure a DVMRP tunnel between two routers.

When a Cisco router runs DVMRP over a tunnel, it advertises sources in DVMRP report messages much as it does on real networks. In addition, the software caches DVMRP report messages it receives and uses them in its Reverse Path Forwarding (RPF) calculation. This behavior allows the software to forward multicast packets received over the tunnel.

When you configure a DVMRP tunnel, you should assign a tunnel an address in the following two cases:

- To enable the sending of IP packets over the tunnel
- To indicate whether the Cisco IOS software should perform DVMRP summarization

You can assign an IP address either by using the **ip address** interface configuration command, or by using the **ip unnumbered** interface configuration command to configure the tunnel to be unnumbered. Either of these two methods allows IP multicast packets to flow over the tunnel. The software will not advertise subnets over the tunnel if the tunnel has a different network number from the subnet. In this case, the software advertises only the network number over the tunnel.

To configure a DVMRP tunnel, use the following commands in interface configuration mode:

SUMMARY STEPS

1. Router(config-if)# **interface tunnel** *number*
2. Router(config-if)# **tunnel source** *ip-address*
3. Router(config-if)# **tunnel destination** *ip-address*
4. Router(config-if)# **tunnel mode dvmrp**
5. Do one of the following:
   - Router(config-if)# **ip address** *address mask*
   -
   -
   - Router(config-if)# **ip unnumbered** *type number*
6. Router(config-if)# **ip pim**[**dense-mode** | **sparse-mode**]
7. Router(config-if)# **ip dvmrp accept-filter** *access-list*[*distance* | **ip neighbor-list** *access-list]*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if)# **interface tunnel** *number*	Specifies a tunnel interface in global configuration mode and puts the router into interface configuration mode.
Step 2	Router(config-if)# **tunnel source** *ip-address*	Sets the source address of the tunnel interface. This address is the IP address of the interface on the router.
Step 3	Router(config-if)# **tunnel destination** *ip-address*	Sets the destination adddress of the tunnel interface. This address is the IP address of the mrouted multitask router.
Step 4	Router(config-if)# **tunnel mode dvmrp**	Configures a DVMRP tunnel.
Step 5	Do one of the following: • Router(config-if)# **ip address** *address mask* • • • Router(config-if)# **ip unnumbered** *type number*	Assigns an IP address to the interface. or Configures the interface as unnumbered.
Step 6	Router(config-if)# **ip pim**[**dense-mode**	**sparse-mode**]	Configures PIM on the interface.
Step 7	Router(config-if)# **ip dvmrp accept-filter** *access-list*[*distance*	**ip neighbor-list** *access-list]*	Configures an acceptance filter for incoming DVMRP reports.

See the "DVMRP Tunnel Example, page 47" section later in this chapter for an example of how to configure a DVMRP tunnel.

Advertising Network 0.0.0.0 to DVMRP Neighbors

The mrouted protocol is a public domain implementation of DVMRP. If your router is a neighbor to an mrouted Version 3.6 device, you can configure the Cisco IOS software to advertise network 0.0.0.0 to the DVMRP neighbor. Do not advertise the DVMRP default into the MBONE. You must specify whether only route 0.0.0.0 is advertised or if other routes can also be specified.

To advertise network 0.0.0.0 to DVMRP neighbors on an interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **ip dvmrp default-information** {**originate** | **only**}	Advertises network 0.0.0.0 to DVMRP neighbors.

Advanced DVMRP Interoperability Configuration Task List

Cisco routers run PIM and know enough about DVMRP to successfully forward multicast packets to receivers and receive multicast packets from senders. It is also possible to propagate DVMRP routes into and through a PIM cloud. PIM uses this information; however, Cisco routers do not implement DVMRP to forward multicast packets.

The basic DVMRP interoperability features are described in the section "Basic DVMRP Interoperability Configuration Task List, page 37" earlier in this chapter. To configure more advanced DVMRP interoperability features on a Cisco router, perform the optional tasks described in the following sections:

- Enabling DVMRP Unicast Routing, page 41 (Optional)
- Limiting the Number of DVMRP Routes Advertised, page 42 (Optional)
- Changing the DVMRP Route Threshold, page 42 (Optional)
- Configuring a DVMRP Summary Address, page 42 (Optional)
- Disabling DVMRP Automatic Summarization, page 43 (Optional)
- Adding a Metric Offset to the DVMRP Route, page 43 (Optional)
- Rejecting a DVMRP Nonpruning Neighbor, page 44 (Optional)
- Configuring a Delay Between DVRMP Reports, page 45 (Optional)

- Enabling DVMRP Unicast Routing, page 41
- Limiting the Number of DVMRP Routes Advertised, page 42
- Changing the DVMRP Route Threshold, page 42
- Configuring a DVMRP Summary Address, page 42
- Disabling DVMRP Automatic Summarization, page 43
- Adding a Metric Offset to the DVMRP Route, page 43
- Rejecting a DVMRP Nonpruning Neighbor, page 44
- Configuring a Delay Between DVRMP Reports, page 45

Enabling DVMRP Unicast Routing

Because policy for multicast routing and unicast routing requires separate topologies, PIM must follow the multicast topology to build loopless distribution trees. Using DVMRP unicast routing, Cisco routers and mrouted machines exchange DVMRP unicast routes, to which PIM can then reverse path forward.

Cisco routers do not perform DVMRP multicast routing among each other, but they can exchange DVMRP routes. The DVMRP routes provide a multicast topology that may differ from the unicast topology. These routes allow PIM to run over the multicast topology, thereby allowing PIM sparse mode over the MBONE topology.

When DVMRP unicast routing is enabled, the router caches routes learned in DVMRP report messages in a DVMRP routing table. PIM prefers DVMRP routes to unicast routes by default, but that preference can be configured.

DVMRP unicast routing can run on all interfaces, including generic routing encapsulation (GRE) tunnels. On DVMRP tunnels, it runs by virtue of DVMRP multicast routing. This feature does not enable DVMRP multicast routing among Cisco routers. However, if there is a DVMRP-capable multicast router, the Cisco router will do PIM/DVMRP multicast routing interaction.

To enable DVMRP unicast routing, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **ip dvmrp unicast-routing**	Enables DVMRP unicast routing.

Limiting the Number of DVMRP Routes Advertised

By default, only 7000 DVMRP routes will be advertised over an interface enabled to run DVMRP (that is, a DVMRP tunnel, an interface where a DVMRP neighbor has been discovered, or an interface configured to run the **ip dvmrp unicast-routing** interface configuration command).

To change this limit, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **ip dvmrp route-limit** *count*	Changes the number of DVMRP routes advertised over an interface enabled to run DVMRP.

Changing the DVMRP Route Threshold

By default, 10,000 DVMRP routes may be received per interface within a 1-minute interval. When that rate is exceeded, a syslog message is issued, warning that a route surge might be occurring. The warning is typically used to quickly detect when routers have been misconfigured to inject a large number of routes into the MBONE.

To change the threshold number of routes that trigger the warning, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **ip dvmrp routehog-notification** *route-count*	Configures the number of routes that trigger a syslog message.

Use the **show ip igmp interface** EXEC command to display a running count of routes. When the count is exceeded, "*** ALERT ***" is appended to the line.

Configuring a DVMRP Summary Address

You can customize the summarization of DVMRP routes if the default classful automatic summarization does not suit your needs. To summarize such routes, specify a summary address by using the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **ip dvmrp summary-address** *summary-address mask* [**metric** *value*]	Specifies a DVMRP summary address.

Note At least one, more-specific route must be present in the unicast routing table before a configured summary address will be advertised.

Disabling DVMRP Automatic Summarization

By default, the Cisco IOS software performs some level of DVMRP summarization automatically. Disable this function if you want to advertise all routes, not just a summary. If you configure the **ip dvmrp summary-address** interface configuration command and did not configure the **no ip dvmrp auto-summary** command, you get both custom and automatic summaries.

To disable DVMRP automatic summarization, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **no ip dvmrp auto-summary**	Disables DVMRP automatic summarization.

Adding a Metric Offset to the DVMRP Route

By default, the router increments by 1 the metric of a DVMRP route advertised in incoming DVMRP reports. You can change the metric if you want to favor or not favor a certain route. The DVMRP metric is a hop count. Therefore, a very slow serial line of one hop is preferred over a route that is two hops over FDDI or another fast medium.

For example, perhaps a route is learned by Router A and the same route is learned by Router B with a higher metric. If you want to use the path through Router B because it is a faster path, you can apply a metric offset to the route learned by Router A to make it larger than the metric learned by Router B, allowing you to choose the path through Router B.

To change the default metric, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **ip dvmrp metric-offset** [**in** | **out**] *increment*	Changes the metric added to DVMRP routes advertised in incoming reports.

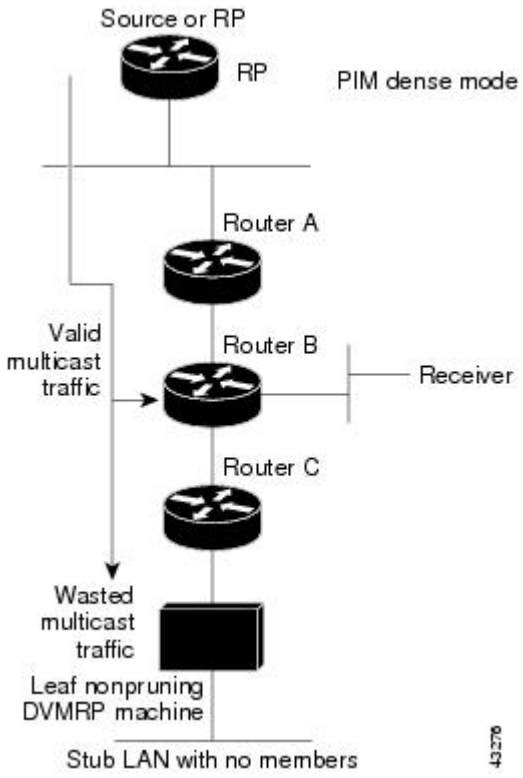
Similar to the **metric** keyword in mrouted configuration files, the following is true when using the **ip dvmrp metric-offset** interface configuration command:

- When you specify the **in**keyword or no keyword, the *increment* value is added to incoming DVMRP reports and is reported in mrinfo replies. The default value for the **in** keyword is 1.
- When you specify the **out** keyword, the *increment* is added to outgoing DVMRP reports for routes from the DVMRP routing table. The default value for the **out** keyword is 0.

Rejecting a DVMRP Nonpruning Neighbor

By default, Cisco routers accept all DVMRP neighbors as peers, regardless of their DVMRP capability or lack of. However, some non-Cisco machines run old versions of DVMRP that cannot prune, so they will continuously receive forwarded packets unnecessarily, wasting bandwidth. The figure shows this scenario.

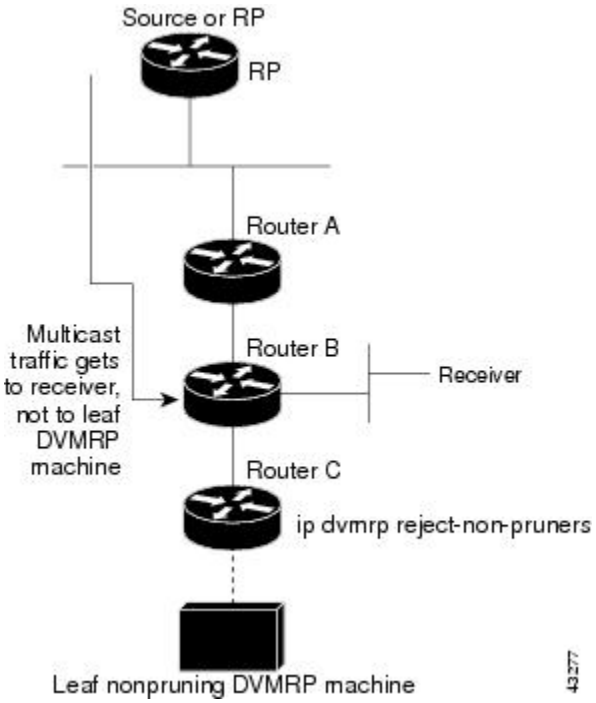
Figure 5



You can prevent a router from peering (communicating) with a DVMRP neighbor if that neighbor does not support DVMRP pruning or grafting. To do so, configure Router C (which is a neighbor to the leaf, nonpruning DVMRP machine) with the **ip dvmrp reject-non-pruners** interface configuration command on the interface to the nonpruning machine. The figure illustrates this scenario. In this case, when the router

receives a DVMRP probe or report message without the Prune-Capable flag set, the router logs a syslog message and discards the message.

Figure 6



Note that the **ip dvmrp reject-non-pruners** command prevents peering with neighbors only. If there are any nonpruning routers multiple hops away (downstream toward potential receivers) that are not rejected, then a nonpruning DVMRP network might still exist.

To prevent peering with nonpruning DVMRP neighbors, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **ip dvmrp reject-non-pruners**	Prevents peering with nonpruning DVMRP neighbors.

Configuring a Delay Between DVRMP Reports

You can configure an interpacket delay of a DVMRP report. The delay is the number of milliseconds that elapse between transmissions of sets of packets that constitute a report. The number of packets in the set is determined by the *burst* value, which defaults to 2 packets. The *milliseconds* value defaults to 100 milliseconds.

To change the default values of the delay, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **ip dvmrp output-report-delay** *milliseconds* `[`*burst*`]`	Configures an interpacket delay between DVMRP reports.

Monitoring and Maintaining DVMRP

To clear routes from the DVMRP routing table, use the following command in EXEC mode:

Command	Purpose
`Router#` **clear ip dvmrp route** `{` ***** `|` *route*`}`	Deletes routes from the DVMRP routing table.

To display entries in the DVMRP routing table, use the following command in EXEC mode:

Command	Purpose
`Router#` **show ip dvmrp route** `[`*name* `|` *ip-address* `|` *type number*`]`	Displays the entries in the DVMRP routing table.

DVMRP Configuration Examples

This section provides the following DVMRP configuration examples:

- DVMRP Interoperability Example, page 46
- DVMRP Tunnel Example, page 47

- DVMRP Interoperability Example, page 46
- DVMRP Tunnel Example, page 47

DVMRP Interoperability Example

The following example configures DVMRP interoperability for configurations when the PIM router and the DVMRP router are on the same network segment. In this example, access list 1 advertises the networks (198.92.35.0, 198.92.36.0, 198.92.37.0, 131.108.0.0, and 150.136.0.0) to the DVMRP router, and access list 2 is used to prevent all other networks from being advertised (the **ip dvmrp metric 0** interface configuration command).

```
interface ethernet 0
 ip address 131.119.244.244 255.255.255.0
 ip pim dense-mode
 ip dvmrp metric 1 list 1
 ip dvmrp metric 0 list 2
access-list 1 permit 198.92.35.0 0.0.0.255
access-list 1 permit 198.92.36.0 0.0.0.255
access-list 1 permit 198.92.37.0 0.0.0.255
access-list 1 permit 131.108.0.0 0.0.255.255
access-list 1 permit 150.136.0.0 0.0.255.255
access-list 1 deny   0.0.0.0 255.255.255.255
access-list 2 permit 0.0.0.0 255.255.255.255
```

DVMRP Tunnel Example

The following example configures a DVMRP tunnel:

```
!
ip multicast-routing
!
interface tunnel 0
 ip unnumbered ethernet 0
 ip pim dense-mode
 tunnel source ethernet 0
 tunnel destination 192.70.92.133
 tunnel mode dvmrp
!
interface ethernet 0
 description Universitat DMZ-ethernet
 ip address 192.76.243.2 255.255.255.0
 ip pim dense-mode
```