Tunneling to Connect Non-IP Multicast Areas

This module describes how to configure a Generic Route Encapsulation (GRE) tunnel to tunnel IP multicast packets between non-IP multicast areas. The benefit is that IP multicast traffic can be sent from a source to a multicast group, over an area where IP multicast is not supported.

Prerequisites for Tunneling to Connect Non-IP Multicast Areas

This module assumes you understand the concepts in the “IP Multicast Technology Overview” module.

Information About Tunneling to Connect Non-IP Multicast Areas

Benefits of Tunneling to Connect Non-IP Multicast Areas

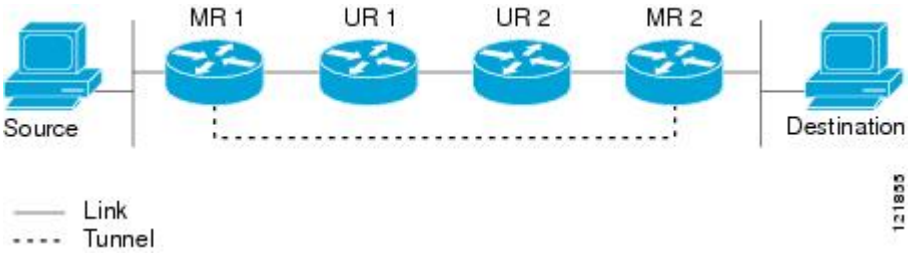
- If the path between a source and a group member (destination) does not support IP multicast, a tunnel between them can transport IP multicast packets.
- Per packet load balancing can be used. Load balancing in IP multicast is normally per (S,G). Therefore, (S1, G) can go over Link X and (S2, G) can go over Link Y, where X and Y are parallel links. If you create a tunnel between the routers, you can get per packet load balancing because the load balancing is done on the tunnel unicast packets.

IP Multicast Static Route

IP multicast static routes (mroutes) allow you to have multicast paths diverge from the unicast paths. When using Protocol Independent Multicast (PIM), the router expects to receive packets on the same interface where it sends unicast packets back to the source. This expectation is beneficial if your multicast and unicast topologies are congruent. However, you might want unicast packets to take one path and multicast packets to take another.

The most common reason for using separate unicast and multicast paths is tunneling. When a path between a source and a destination does not support multicast routing, a solution is to configure two routers with a GRE tunnel between them. In the figure, each unicast router (UR) supports unicast packets only; each multicast router (MR) supports multicast packets.

Figure 1: Tunnel for Multicast Packets



In the figure, Source delivers multicast packets to Destination by using MR 1 and MR 2. MR 2 accepts the multicast packet only if it believes it can reach Source over the tunnel. If this situation is true, when Destination sends unicast packets to Source, MR 2 sends them over the tunnel. The check that MR2 can reach Source over the tunnel is a Reverse Path Forwarding (RPF) check, and the static mroute allows the check to be successful when the interface that the multicast packet arrives on is not the unicast path back to the source. Sending the packet over the tunnel could be slower than natively sending it through UR 2, UR 1, and MR 1.

A multicast static route allows you to use the configuration in the figure by configuring a static multicast source. The system uses the configuration information instead of the unicast routing table to route the traffic. Therefore, multicast packets can use the tunnel without having unicast packets use the tunnel. Static mroutes are local to the router they are configured on and not advertised or redistributed in any way to any other router.

How to Connect Non-IP Multicast Areas

Configuring a Tunnel to Connect Non-IP Multicast Areas

Configure a multicast static route if you want your multicast paths to differ from your unicast paths. For example, you might have a tunnel between two routers because the unicast path between a source and destination does not support multicast routing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip unnumbered** *type number*
5. **ip pim sparse-mode**
6. **tunnel source** {*ip-address* | *type number*}
7. **tunnel destination** {*hostname* | *ip-address*}
8. Repeat Steps 1 through 7 on the router at the opposite end of the tunnel, reversing the tunnel source and destination addresses.
9. **end**
10. **ip mroute** *source-address mask* **tunnel** *number* [*distance*]

11. **ip mroute** *source-address mask* **tunnel** *number* [*distance*]
12. **end**
13. **show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*]
14. **show ip rpf** {*source-address* | *source-name*} [**metric**]

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 tunnel** *number* **Example:** `Router(config)# interface tunnel 0`	Configures a tunnel interface.
Step 4	**ip unnumbered** *type number* **Example:** `Router(config-if)# ip unnumbered gigabitethernet 0/0/0`	Enables IP processing without assigning an IP address to the interface.
Step 5	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on the tunnel interface.
Step 6	**tunnel source** {*ip-address* | *type number*} **Example:** `Router(config-if)# tunnel source 100.1.1.1`	Configures the tunnel source.
Step 7	**tunnel destination** {*hostname* | *ip-address*} **Example:** `Router(config-if)# tunnel destination 100.1.5.3`	Configures the tunnel destination.
Step 8	Repeat Steps 1 through 7 on the router at the opposite end of the tunnel, reversing the tunnel source and destination addresses.	Router A's tunnel source address will match Router B's tunnel destination address. Router A's tunnel destination address will match Router B's tunnel source address.

	Command or Action	Purpose
Step 9	**end** **Example:** `Router(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 10	**ip mroute** *source-address mask* **tunnel** *number* [*distance*] **Example:** `Router(config)# ip mroute 0.0.0.0 0.0.0.0 tunnel 0`	Configures a static multicast route over which to reverse path forward to the other end of the tunnel. • Because the use of the tunnel makes the multicast topology incongruent with the unicast topology, and only multicast traffic traverses the tunnel, you must configure the routers to reverse path forward correctly over the tunnel. • When a source range is specified, the mroute applies only to those sources. • In the example, the *source-address* and *mask* of 0.0.0.0 0.0.0.0 indicate any address. • The shorter distance is preferred. • The default distance is 0.
Step 11	**ip mroute** *source-address mask* **tunnel** *number* [*distance*] **Example:** `Router(config)# ip mroute 0.0.0.0 0.0.0.0 tunnel 0`	Configures a static route over which to reverse path forward from the access router to the other end of the tunnel.
Step 12	**end** **Example:** `Router(config)# end`	(Optional) Ends the current configuration session and returns to privileged EXEC mode.
Step 13	**show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*] **Example:** `Router# show ip mroute`	(Optional) Displays the contents of the IP multicast routing (mroute) table.
Step 14	**show ip rpf** {*source-address* | *source-name*} [**metric**] **Example:** `Router# show ip rpf 10.2.3.4`	(Optional) Displays how IP multicast routing does RPF.

Configuration Examples for Tunneling to Connect Non-IP Multicast Areas

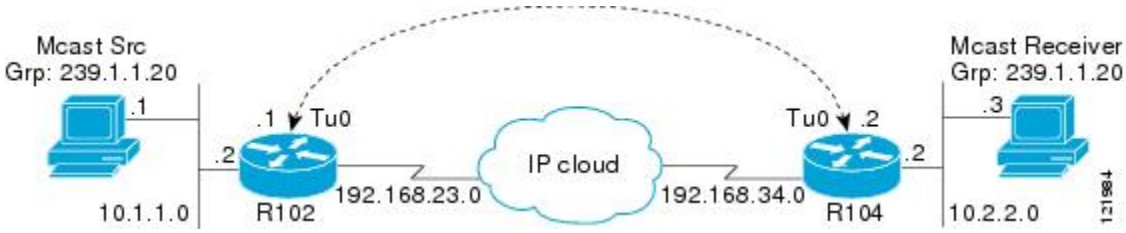
Tunneling to Connect Non-IP Multicast Areas Example

The following example also appears online at:

http://www.cisco.com/en/US/tech/tk828/tk363/technologies_configuration_example09186a00801a5aa2.shtml

In the figure below, the multicast source (10.1.1.1) is connected to R102 and is configured for multicast group 239.1.1.20. The multicast receiver (10.2.2.3) is connected to R104 and is configured to receive multicast packets for group 239.1.1.20. Separating R102 and R104 is an IP cloud, which is not configured for multicast routing.

Figure 2: Tunnel Connecting Non-IP Multicast Areas



A tunnel is configured between R102 to R104 sourced with their loopback interfaces. The **ip pim sparse-dense-mode** command is configured on tunnel interfaces and multicast-routing is enabled on R102 and R104. Sparse-dense mode configuration on the tunnel interfaces allows sparse-mode or dense-mode packets to be forwarded over the tunnel depending on rendezvous point (RP) configuration for the group.

Note For dense mode--With PIM dense mode configured over the tunnel, an **ip mroute 10.1.1.0 255.255.255.0 tunnel 0** command is configured on R104 to ensure a successful RPF for multicast source address 10.1.1.1. Incoming (10.1.1.1, 239.1.1.20) multicast packets over Tunnel0 (Tu0) are checked for Reverse Path Forwarding (RPF) using this mroute statement. After a successful check, the multicast packets are forwarded to outgoing interface list (OIL) interfaces.

Note For sparse mode--With PIM sparse mode configured over the tunnel, ensure that the following points are addressed:

- For a successful RPF verification of multicast traffic flowing over the shared tree (*,G) from RP, an **ip mroute rp-address nexthop** command needs to be configured for the RP address, pointing to the tunnel interface.

Assuming R102 to be the RP (RP address 2.2.2.2) in this case, the mroute would be the **ip mroute 2.2.2.2 255.255.255.255 tunnel 0**command, which ensures a successful RPF check for traffic flowing over the shared tree.

- For a successful RPF verification of multicast (S,G) traffic flowing over the Shortest Path Tree (SPT), an **ip mroute source-address nexthop** command needs to be configured for the multicast source, pointing to the tunnel interface.

In this case, when SPT traffic is flowing over tunnel interface an **ip mroute 10.1.1.0 255.255.255.0 tunnel 0** command is configured on R104 to ensure a successful RPF verification for incoming (10.1.1.1, 239.1.1.20) multicast packets over the Tunnel 0 interface.

R102#

```
version 12.2
hostname r102
ip subnet-zero
no ip domain-lookup
!--- It stops IP domain lookup, which improves the show command response time.
!
ip multicast-routing
!--- Enables IP multicast routing.
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!--- Tunnel Source interface.
!
interface Tunnel0
!--- Tunnel interface configured for PIM and carrying multicast packets to R104.
 ip address 192.168.24.1 255.255.255.252
 ip pim sparse-dense-mode
 tunnel source Loopback0
 tunnel destination 4.4.4.4
!
interface Ethernet0/0
!--- Interface connected to Source.
ip address 10.1.1.2 255.255.255.0
 ip pim sparse-dense-mode
!
interface Serial8/0
 ip address 192.168.23.1 255.255.255.252
!--- Note IP PIM sparse-dense mode is not configured on Serial interface.
!
router ospf 1
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 10.1.1.0 0.0.0.255 area 0
 network 192.168.23.0 0.0.0.255 area 0
!
ip classless
ip pim bidir-enable
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

R104#

```
version 12.2
!
hostname r104
```

```
!
ip subnet-zero
no ip domain-lookup
!--- It stops IP domain lookup, which improves the show command response time.
!
ip multicast-routing
!--- Enables IP multicast routing.
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
!--- Tunnel Source interface.
!
interface Tunnel0
 ip address 192.168.24.2 255.255.255.252
!--- Tunnel interface configured for PIM and carrying multicast packets.
ip pim sparse-dense-mode
 tunnel source Loopback0
 tunnel destination 2.2.2.2
!
interface Ethernet0/0
 ip address 10.2.2.2 255.255.255.0
 ip pim sparse-dense-mode
!
interface Serial9/0
 ip address 192.168.34.1 255.255.255.252
!--- Note IP PIM sparse-dense mode is not configured on Serial interface.
!
!
router ospf 1
 log-adjacency-changes
 network 4.4.4.4 0.0.0.0 area 0
 network 10.2.2.0 0.0.0.255 area 0
 network 192.168.34.0 0.0.0.255 area 0
!
ip classless
no ip http server
ip pim bidir-enable
ip mroute 10.1.1.0 255.255.255.0 Tunnel0
!--- This Mroute ensures a successful RPF check for packets flowing from the source.
!--- 10.1.1.1 over Shared tree in case of Dense more and SPT in case of Sparse mode.
!
ip mroute 2.2.2.2 255.255.255.255 tunnel 0
!--- This Mroute is required for RPF check when Sparse mode multicast traffic is
!--- flowing from RP (assuming R102 with 2.2.2.2 as RP)  towards receiver via tunnel
!--- before the SPT switchover.
line con 0
line aux 0
line vty 0 4
 login
!
end
```

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
None	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing standards has not been modified by this feature.	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
None	--

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 Tunneling to Connect Non-IP Multicast Areas

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 https://cfnng.cisco.com/. An account on Cisco.com is not required.