

Multicast over a GRE Tunnel

Document ID: 43584

Introduction

Prerequisites

Requirements

Components Used

Conventions

Configure

Network Diagram

Configurations

Verify

Troubleshoot

Related Information

Introduction

This document provides a sample configuration for multicasting over a generic routing encapsulation (GRE) tunnel.

In many network scenarios you want to configure your network to use GRE tunnels to send Protocol Independent Multicast (PIM) and multicast traffic between routers. Typically, this occurs when the multicast source and receiver are separated by an IP cloud which is not configured for IP multicast routing. In such network scenarios, configuring a tunnel across an IP cloud with PIM enabled transports multicast packets toward the receiver. This document describes the configuration, verification, and related issues pertaining to multicasting over a GRE tunnel.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- A basic understanding of multicast and PIM is helpful. Refer to the Multicast Quick-Start Configuration Guide for more information on multicast and PIM.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

As the network diagram shows, 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.

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 these 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, that points to the tunnel interface.

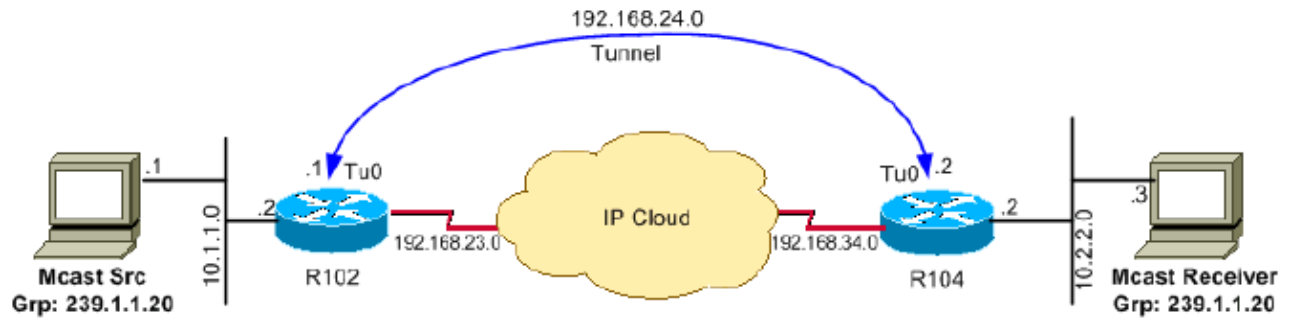
With the assumption that R102 is the RP (RP address 2.2.2.2) in this case, then the mroute is the **ip mroute 2.2.2.2 255.255.255.255 tunnel 0** command, which ensures a successful RPF check for traffic that flows over the shared tree.

- 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 Tu0 interface.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- R102
- R104

Configure Router 102 according to this running configuration file:

```

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

```

Configure Router 104 according to this running configuration file:

R104
<pre> 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 </pre>

```

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

```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show ip igmp group** Verifies that the receiver has sent its IGMP join membership request for group 239.1.1.20 to R104.

```

r104#show ip igmp groups
IGMP Connected Group Membership
Group Address      Interface          Uptime    Expires    Last Reporter
239.1.1.20         Ethernet0/0       00:00:04  00:02:55  10.2.2.3

```

- **show ip mroute group-address** Verifies that when the source 10.1.1.1 starts multicasting packets for the group 239.1.1.20, R102 installs the (*,239.1.1.20) and (10.1.1.1, 239.1.1.20) entries in the

R102 mroute table.

Note: In the (10.1.1.1, 239.1.1.20) entry, the OIL is Tunnel0.

```
r102#show ip mroute 239.1.1.20
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
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.1.1.20), 00:00:09/00:02:59, RP 0.0.0.0, flags: D
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 00:00:09/00:00:00
    Ethernet0/0, Forward/Sparse-Dense, 00:00:09/00:00:00

(10.1.1.1, 239.1.1.20), 00:00:09/00:02:58, flags: T
  Incoming interface: Ethernet0/0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 00:00:09/00:00:00
```

- **show ip mroute group-address** Verifies that R104 has the (*,239.1.1.20) and (10.1.1.1, 239.1.1.20) entries while it is forwarding multicast packets for group 239.1.1.20 sourced from 10.1.1.1.

Note: In (10.1.1.1, 239.1.1.20), the incoming interface is Tunnel0 and the RPF neighbor is 192.168.24.1 the Tunnel head end on R102. The RPF verification is done based on the mroute configured on R104, and the multicast packets are pushed out to the OIL to the receiver connected on the Ethernet 0/0 interface.

```
r104#show ip mroute 239.1.1.20
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
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.1.1.20), 00:07:10/00:00:00, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 00:07:10/00:00:00
    Ethernet0/0, Forward/Sparse-Dense, 00:07:10/00:00:00

(10.1.1.1, 239.1.1.20), 00:01:13/00:02:24, flags: CLT
  Incoming interface: Tunnel0, RPF nbr 192.168.24.1, Mroute
  Outgoing interface list:
    Ethernet0/0, Forward/Sparse-Dense, 00:01:13/00:00:00
```

- **show ip rpf ip-address** Perform an RPF verification for packets sourced from 10.1.1.1. The following example confirms that RPF for 10.1.1.1 is via Tunnel 0, on which we are receiving the multicast (S,G) packets.

```
r104>show ip rpf 10.1.1.1
RPF information for ? (10.1.1.1)
RPF interface: Tunnel0
```

```
RPF neighbor: ? (192.168.24.1)
RPF route/mask: 10.1.1.1/24
RPF type: static
RPF recursion count: 0
Doing distance-preferred lookups across tables
```

Troubleshoot

Use this section to troubleshoot your configuration.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

If your multicast over GRE tunnel is not working, one of these can be the cause:

- **Tunnel not UP/UP** The tunnel source and destination do not match on each end of the tunnel. For example, if the tunnel destination on R102 was changed to the IP address 10.2.2.2 instead of 2.2.2.2 while the configuration on R104 remained the same, the tunnel would not come up.

Issue the **show interface tunnel 0** command in order to verify the status of the tunnel.

- **Multicast packets are dropped because of RPF failure.**

Issue the **show ip mroute count** command. A sample output of this command and its increasing counters for RPF failure is shown in this output:

```
r104#show ip mroute count
IP Multicast Statistics
3 routes using 1642 bytes of memory
2 groups, 0.50 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 224.0.1.40, Source count: 0, Packets forwarded: 0, Packets received: 0

Group: 239.1.1.20, Source count: 1, Packets forwarded: 11, Packets received: 45
Source: 10.1.1.1/32, Forwarding: 11/0/100/0, Other: 25/14/0
```

*!--- After some time, the show ip mroute count command
!--- is issued again. You can see the RPF failed counter increasing:*

```
r104#show ip mroute count
IP Multicast Statistics
3 routes using 1642 bytes of memory
2 groups, 0.50 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 224.0.1.40, Source count: 0, Packets forwarded: 0, Packets received: 0

Group: 239.1.1.20, Source count: 1, Packets forwarded: 11, Packets received: 50
Source: 10.1.1.1/32, Forwarding: 11/0/100/0, Other: 30/19/0
r104#
```

You can also issue the **show ip rpf source** command. Ensure that the RPF interface is the same as that on which the source multicast packets are received Tunnel 0 in this example. Refer to the IP

Multicast Troubleshooting Guide for more information about RPF failures.

- **PIM Neighbors** Router R102 is not forwarding over the Tunnel0 interface because it is not seeing a PM neighbor R104.

Issue these commands:

- ◆ **show ip pim neighbor** You can use the **show ip pim neighbor** command on R102 to show the neighbor R104 over the tunnel.
- ◆ **show ip pim int** You can also use the **show ip pim int** command to show that there is a neighbor.
- ◆ **ip pim sparse-dense-mode** Verify that the interface level **ip pim sparse-dense-mode** command is configured on both ends of the tunnel and that IP multicast-routing is enabled.

Related Information

- [Multicast Quick-Start Configuration Guide](#)
- [IP Multicast Troubleshooting Guide](#)
- [Basic Multicast Troubleshooting Tools](#)
- [TCP/IP Multicast Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Mar 06, 2007

Document ID: 43584
