Automatic Multicast Tunneling

Automatic Multicast Tunneling (AMT) provides a method to tunnel multicast data over a unicast network. The tunneling is performed between AMT relays and AMT gateways, using User Datagram Protocol (UDP) encapsulation. AMT enables service providers and their customers to participate in delivering multicast traffic even in the absence of end-to-end multicast connectivity.

- Finding Feature Information, page 1
- Restrictions for Automatic Multicast Tunneling, page 1
- Information About Automatic Multicast Tunneling, page 2
- How to Configure Automatic Multicast Tunneling, page 4
- Configuration Examples for Automatic Multicast Tunneling, page 17
- Additional References for Automatic Multicast Tunneling, page 18
- Feature Information for Automatic Multicast Tunneling, page 18

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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 Automatic Multicast Tunneling

- AMT tunnel only support PIM passive mode on AMT Gateway side.
- AMT only support SSM modes for PIM signaling.
- AMT only support ipv4 transport for tunnel.
- For AMT, auto-rp is invalid between relay and gateway.
Information About Automatic Multicast Tunneling

Overview

The multicast source sends traffic to the first-hop. Multicast traffic flows through the network until it reaches the last-hop (receivers) or AMT relays. AMT Relay is a multicast router configured to support transit routing between non-multicast capable internetwork and the native multicast infrastructure.

The following diagram provides a sample AMT network where Relay1 and Relay2 are two AMT relays, which encapsulate the traffic into AMT tunnels, and send one copy to each of the AMT gateways.

Figure 1: Automatic Multicast Tunneling (AMT)

Automatic Multicast Tunneling Message Exchanges

The AMT protocol defines seven message types for control and encapsulation. The message exchanges happen in the following sequence:

1. **Relay Discovery**—Gateway sends an AMT discovery message to an anycast address that represents the AMT relay.
2. **Relay Advertisement**—Relay responds with an advertisement message, which includes the relay’s unique IP address.
3. **Relay Request**—Gateway sends an AMT Request message to the relay using the unique IP address as the destination, along with a nonce to be used for security.
4. **Membership Query**—Relay responds with an AMT query that includes the nonce from the AMT request and an opaque security code.
5. **Membership Update**—Gateway responds with a membership update that includes an encapsulated IGMPv3/MLDv2 packet.
Teardown—Gateway sends a message to stop the delivery of multicast data messages requested in an earlier membership update message.

After validation the Relay establishes the AMT Tunnel and starts sending multicast traffic [Type 6]. Any further (S,G) uses the same Request/Query/Update - three-way handshake because the tunnel is already established.

**AMT Tunnel and Traffic Types**

The multicast traffic carried in the AMT tunnel may be IPv4 or IPv6. The AMT tunnel may be setup with IPv4 or IPv6 endpoints, thereby providing the following possibilities.

- IPv4-in-IPv4—IPv4 multicast traffic carried over an IPv4 tunnel
- IPv6-in-IPv4—IPv6 multicast traffic carried over an IPv4 tunnel
- IPv6-in-IPv6—IPv6 multicast traffic carried over an IPv6 tunnel
- IPv4-in-IPv6—IPv4 multicast traffic carried over an IPv6 tunnel

**Note**

In Cisco IOS XE Release 3.15S, AMT supports IPv4-in-IPv4 and IPv6-in-IPv4 only.

**Advantages of Automatic Multicast Tunneling**

- Simplicity—Instead of incurring the overhead of manually provisioning, establishing and maintaining GRE tunnels between two locations, the receiving network simply sends AMT advertisements to a well-known any-cast prefix. The rest of the tunnel establishment process is done automatically without the need for additional configuration.
- Resiliency—Because the relay discovery uses an any-cast address, gateways automatically find the closest relay. If that relay becomes unavailable or unreachable, the routing table reconverges on the next closest relay.
- Efficiency—AMT allows transit routers to perform flow-based load balancing for more efficient link utilization.

Automatic Multicast Tunneling supports IPv4 transport for tunnel and also support for IPv4 multicast traffic & IPv6 multicast traffic. You can also configure AMT relay-only, gateway-only and relay-gateway coexisting modes.

**Prerequisites for AMT**

- AMT relay and gateway tunnel requires an interface IP address. However the interface IP addresses do not need to be unique. You can configure the same addresses for the tunnel source address using the `ip unnumbered` command.
- You must configure IGMP version 3 on the tunnel interfaces for the SSM to work across tunnels.
The tunnel source port and tunnel destination port must be configured to achieve a valid AMT configuration.

Configuration Recommendations for AMT

The tunnel source interface address should be an interface that is set up to be reachable from receivers under all instances. You can use a physical interface address, but it can cause the tunnel to go down if that physical interface is down. A loopback interface is recommended to sustain availability. You do not need a separate loopback address, you can reuse the loopback interface that you usually would have to carry router and router-ID IP address (usually Loopback 0).

IP PIM passive is the recommended and supported mode on AMT interfaces to enable IP multicast routing for AMT tunnel interfaces. This is recommended since no PIM messages (only AMT/IGMP messages) will be sent or received via the AMT tunnel.

On an AMT relay, you need only one tunnel interface to which all gateways can connect. Therefore the interface is a multipoint interface. Every gateway interface can only connect to one relay, but you can configure multiple tunnel interfaces.

Even though AMT tunnels (relay and gateway) only support IPv4 tunnels, the IPv4 tunnels can carry both IPv4 and IPv6 simultaneously. You can configure the AMT for the version(s) of IP that you need.

If you want to set up a redundant AMT relay, your AMT relay address configured on the gateway should be any IP address that you set up as an anycast address on your relays. If you do not plan to use redundant (Anycast) Relay, you can use the relays tunnel source address on the gateways.

If you shut down the anycast Loopback interface, the AMT relay would not accept new AMT gateway tunnel requests. IP routing for the anycast address would only point to any other relays active with the same address and new requests would therefore go to those relays. Any AMT gateways already connected to this relay would stay on this relay, because they already are using the relays interface address.

How to Configure Automatic Multicast Tunneling

Enabling and Configuring Automatic Multicast Tunneling on a Relay

Note
Switch-over from active relay to backup relay can take more than 5 minutes.
**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface tunnel number`
4. `ip address ip-address mask`
5. `no ip redirects`
6. `ip pim sparse-mode`
7. `ip igmp version version number`
8. `ipv6 enable`
9. `tunnel source interface-type interface-number`
10. `tunnel mode udp multipoint`
11. `tunnel dst-port dynamic`
12. `tunnel src-port dynamic`
13. `amt relay traffic {ip | ipv6}`
14. `exit`
15. `ip multicast-routing distributed`
16. `ipv6 multicast-routing`
17. `ip pim ssm {default | range access-list}`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Device# configure terminal | |

| **Step 3** interface tunnel number | Specifies the interface tunnel number and enters interface configuration mode. |
| **Example:** Device(config)# interface tunnel 11 | |

| **Step 4** ip address ip-address mask | Configures the IP address on the interface. |
| **Example:** Device(config-if)# 11.1.1.1 255.255.255.0 | |

<p>| <strong>Step 5</strong> no ip redirects | Disables sending ICMP Redirect messages. |
| <strong>Example:</strong> Device(config-if)# no ip redirects | |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td><code>ip pim sparse-mode</code></td>
<td>Enable PIM sparse-mode operation.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-if)# ip pim sparse-mode</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>ip igmp version version number</code></td>
<td>Specifies IGMP version.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-if)# ip igmp version 3</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>ipv6 enable</code></td>
<td>Enables IPv6 on interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-if)# ipv6 enable</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>tunnel source interface-type interface-number</code></td>
<td>Configures tunnel source as a loopback interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-if)# tunnel source loopback 0</code></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><code>tunnel mode udp multipoint</code></td>
<td>Specifies the UDP encapsulation protocol.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-if)# tunnel mode udp multipoint</code></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td><code>tunnel dst-port dynamic</code></td>
<td>Specifies the tunnel destination port.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-if)# tunnel dst-port dynamic</code></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td><code>tunnel src-port dynamic</code></td>
<td>Specifies the tunnel source port.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-if)# tunnel src-port dynamic</code></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>`amt relay traffic {ip</td>
<td>ipv6}`</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-if)# amt relay traffic ipv6</code></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td><code>exit</code></td>
<td>Exits interface configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-if)# exit</code></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td><code>ip multicast-routing distributed</code></td>
<td>Enables Multicast Distributed Switching (MDS).</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# ip multicast-routing distributed</code></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td><code>ipv6 multicast-routing</code></td>
<td>Enables multicast routing using Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD).</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# ipv6 multicast-routing</code></td>
<td></td>
</tr>
</tbody>
</table>
Enabling and Configuring Automatic Multicast Tunneling on Gateway

SUMMARY STEPS

1. enable
2. configure terminal
3. interface tunnel number
4. ip address ip-address mask
5. ip pim passive
6. ip igmp version version number
7. ipv6 enable
8. ipv6 pim passive
9. tunnel source interface-type interface-number
10. tunnel mode udp ip
11. tunnel destination dynamic
12. tunnel dst-port dynamic
13. tunnel src-port dynamic
14. amt gateway traffic {ip | ipv6}
15. amt gateway relay-address IP address
16. exit
17. ip multicast-routing distributed
18. ipv6 multicast-routing
19. ip pim ssm {default | range access-list}
20. ipv6 multicast pim-passive-enable
21. ip route ip-address interface-type interface-number [multicast]
22. ipv6 route ipv6-prefix/prefix-length interface-type interface-number [multicast]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Device&gt; enable</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device# configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies the interface tunnel number and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>interface tunnel</strong> <strong>number</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device(config)# interface tunnel 11</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures the IP address on the interface.</td>
</tr>
<tr>
<td><strong>ip address</strong> <strong>ip-address</strong> <strong>mask</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device(config-if)# 11.1.1.1 255.255.255.0</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Enables IP PIM passive mode operation.</td>
</tr>
<tr>
<td><strong>ip pim passive</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device(config-if)# ip pim passive</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Specifies IGMP version.</td>
</tr>
<tr>
<td><strong>ip igmp version</strong> <strong>version number</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device(config-if)# ip igmp version 3</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Enables IPv6 on interface.</td>
</tr>
<tr>
<td><strong>ipv6 enable</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device(config-if)# ipv6 enable</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Enables IPv6 PIM passive mode operation.</td>
</tr>
<tr>
<td><strong>ipv6 pim passive</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device(config-if)# ipv6 pim passive</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Configures tunnel source as a loopback interface.</td>
</tr>
<tr>
<td><strong>tunnel source</strong> <strong>interface-type</strong> <strong>interface-number</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device(config-if)# tunnel source loopback 0</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Specifies the UDP encapsulation protocol.</td>
</tr>
<tr>
<td><strong>tunnel mode udp ip</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device(config-if)# tunnel mode udp ip</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Applies the tunnel destination address dynamically to the tunnel interface.</td>
</tr>
<tr>
<td><strong>tunnel destination dynamic</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device(config-if)# tunnel destination dynamic</strong></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>12</td>
<td>tunnel dst-port dynamic</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# tunnel dst-port dynamic</td>
</tr>
<tr>
<td>13</td>
<td>tunnel src-port dynamic</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# tunnel src-port dynamic</td>
</tr>
<tr>
<td>14</td>
<td>amt gateway traffic {ip</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# amt gateway traffic ipv6</td>
</tr>
<tr>
<td>15</td>
<td>amt gateway relay-address IP address</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# amt gateway relay-address 172.16.0.0</td>
</tr>
<tr>
<td>16</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# exit</td>
</tr>
<tr>
<td>17</td>
<td>ip multicast-routing distributed</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip multicast-routing distributed</td>
</tr>
<tr>
<td>18</td>
<td>ipv6 multicast-routing</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# ipv6 multicast-routing</td>
</tr>
<tr>
<td>19</td>
<td>ip pim ssm {default</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip pim ssm default</td>
</tr>
<tr>
<td>20</td>
<td>ipv6 multicast pim-passive-enable</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# ipv6 multicast pim-passive-enable</td>
</tr>
<tr>
<td>21</td>
<td>ip route ip-address interface-type interface-number [multicast]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip route 101.0.0.2 255.255.255.255 tunnel10 multicast</td>
</tr>
</tbody>
</table>
### Purpose

Command or Action | Purpose
--- | ---
**Step 22** | ipv6 route ipv6-prefix/prefix-length interface-type interface-number [multicast] | Specifies the IPv6 prefix and length along with interface type, interface number, and multicast route (route only usable by multicast).

**Example:**
Device(config)# ipv6 route 2011::101:0:0:2/128 Tunnel10 multicast

### Displaying and Verifying AMT Configuration

**Before You Begin**

#### SUMMARY STEPS

1. ping 3.3.3.3 source 5.5.5.5
2. show ip igmp membership
3. show ip mroute
4. show ip rpf 10.3.3.1

#### DETAILED STEPS

**Step 1**
**ping 3.3.3.3 source 5.5.5.5**

**Example:**
Device# ping 3.3.3.3 source 5.5.5.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 5.5.5.5
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/8 ms

Ping the relay tunnel source address from the gateway, using the gateways tunnel source address and the gateway address (if both are different as the example).

**Step 2**
**show ip igmp membership**

**Example:**
Device# show ip igmp membership

<table>
<thead>
<tr>
<th>Channel/Group</th>
<th>Reporter</th>
<th>Uptime</th>
<th>Exp.</th>
<th>Flags</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>/*,232.2.3.4</td>
<td>0.0.0.0</td>
<td>00:03:02</td>
<td>stop</td>
<td>2MA</td>
<td>Lo0</td>
</tr>
<tr>
<td>10.3.3.1,232.2.3.4</td>
<td>00:03:02</td>
<td>stop</td>
<td>A</td>
<td>Lo0</td>
<td></td>
</tr>
</tbody>
</table>

**Note** The command is executed at destination gateway.

You can use the **ip igmp static-group** command, you create an IGMP membership request on the interface. You can do this on any physical interface configured for IP multicast, but if there are multiple routers attached to the interface, then the AMT gateway router may not become the PIM-DR and therefore not join to the multicast traffic. It can therefore be easier to put the join on an existing loopback interface and also enable it for IP multicast (IP PIM passive).
Step 3  show ip mroute

Example:
Device# show ip mroute
   ... 
   (10.3.3.1, 232.2.3.4), 00:01:53/00:01:08, flags: sTI
     Incoming interface: Tunnel1, RPF nbr 0.0.0.0, Mroute
     Outgoing interface list:
     Loopback0, Forward/Sparse-Dense, 00:01:51/00:01:08

Note  The command is executed at destination gateway.

The AMT gateway will join the multicast traffic towards the AMT relay if the mroute shows the incoming interface as the Tunnel interface and when it is joined for example, when there are one or more outgoing interfaces. When the command is executed on the source gateway, the mroute state on the relay will show the relay interface as an adjacency in the outgoing interface list. Because there is one interface for all joining relays, each outgoing copy across the AMT relay interface is identified by the AMT relay interface, the IP address of the gateway and the UDP port number of the relay as seen by the relay. If there are multiple gateways in a home behind a NAT/PAT (single IP address to the internet), there would be multiple adjacencies shown with the same gateway IP address, but different UDP ports. If state is not built as expected, you can use **debug ip igmp** to troubleshoot it. There are no additional AMT debugs for the AMT/IGMP joins, instead those are all part of IGMP debugs.

Step 4  show ip rpf/10.3.3.1

Example:
Device# show ip rpf/10.3.3.1
   RPF information for ? (10.3.3.1)
   RPF interface: Tunnel1
   RPF neighbor: ? (0.0.0.0)
   RPF route/mask: 10.3.3.0/24
   RPF type: multicast (static)
   Doing distance-preferred lookups across tables
   RPF topology: ipv4 multicast base

Note  The command is executed at destination gateway.

Verifies Multicast RPF.

If the output is not showing the desired AMT gateway tunnel interface as the RPF interface, then your routing configuration for IP multicast into the AMT tunnel is not set up correctly. If you have only one AMT gateway interface, you can use a static mroute. If you have multiple AMT tunnel for different relays, you need to configure the source prefixes (and RP-addresses when you use PIM-SM) towards their respective AMT tunnel.

For IP multicast tree to flow correctly via the AMT tunnels, you must first check if the IP multicast state is correctly built from gateway to relay. This primarily means that the (S,G) join for a source in PIM-SSM/PIM-SM or the (*,G) join to the RP address in PIM-SM need to RPF towards the desired AMT gateway tunnel.
Displaying and Verifying AMT Relay Configuration

SUMMARY STEPS

1. enable
2. show ip amt tunnel
3. show ip mroute section [group-address]
4. show ipv6 mroute section [group-address]
5. show ip mfib section [group-address]
6. show ipv6 mfib section [group-address]
7. show platform software ip rp active mfib section [group-address]
8. show platform software ipv6 rp active mfib section [group-address]
9. show platform software mlist rp active index multicast-index-number
10. show platform software adjacency rp active index platform-allocated-index-value
11. show ip interface brief

DETAILED STEPS

Step 1 enable

Example:
Device> enable
Enables privileged EXEC mode.
  • Enter your password if prompted.

Step 2 show ip amt tunnel

Example:
Device# show ip amt tunnel
AMT Relay tunnel:
  Local address       UDP port
11.11.11.11          2268 (0x8DC )
  Remote address      Expire time
33.33.33.33          59464 (0xE848) 00:03:07
Connected to 1 Gateway
Total active Gateways: 1
Displays AMT relay configuration.

Step 3 show ip mroute section [group-address]

Example:
Device# show ip mroute section 232.1.1.1
(101.0.0.2, 232.1.1.1), 2d00h/00:02:18, flags: stI
  Incoming interface: GigabitEthernet0/0/4, RPF nbr 0.0.0.0
  Outgoing interface list:
    Tunnel10, 33.33.33.33, UDP port 59464, Forward/Sparse, 2d00h/00:02:18
Displays information about sparse mode routes in the IP multicast routing (mroute) table for the specified multicast group.

**Step 4**

```
show ipv6 mroute section [group-address]
```

**Example:**

```
Device# show ipv6 mroute section 232.1.1.1
```

```
(2011::101:0:0:2, FF3F::232:1:1:1), 2d00h/never, flags: sTI
Incoming interface: GigabitEthernet0/0/4
RPF nbr: 2011::101:0:0:2
Immediate outgoing interface list:
    Tunnel10, AMT NH 33.33.33.33, UDP Port 59464, Forward, 2d00h/never
```

Displays information about sparse mode routes in the IPv6 mroute table for the specified multicast group.

**Step 5**

```
show ip mfib section [group-address]
```

**Example:**

```
Device# show ip mfib section 232.1.1.1
```

```
(101.0.0.2,232.1.1.1) Flags: HW
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding: NA/NA/NA/NA, Other: NA/NA/NA
  GigabitEthernet0/0/4 Flags: A
  Tunnel10, AMT Encap 33.33.33.33, UDP Port:59464 Flags: F NS
  Pkts: 0/0
```

Displays the status of entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB) for the specified multicast group.

**Step 6**

```
show ipv6 mfib section [group-address]
```

**Example:**

```
Device# show ipv6 mfib section 232.1.1.1
```

```
(2011::101:0:0:2,FF3F::232:1:1:1) Flags: HW
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding: NA/NA/NA/NA, Other: NA/NA/NA
  GigabitEthernet0/0/4 Flags: A
  Tunnel10, AMT Encap 33.33.33.33, UDP Port:59464 Flags: F NS
  Pkts: 0/0
```

Displays the status of entries and interfaces in the IPv6 Multicast Forwarding Information Base (MFIB) for the specified multicast group.

**Step 7**

```
show platform software ip rp active mfib section [group-address]
```

**Example:**

```
Device# show platform software ip rp active mfib section 232.1.1.1
```

```
232.1.1.1, 101.0.0.2/64 --> OBJ_INTF_LIST (0x5a)
  Obj id: 0x5a, Flags:
    OM handle: 0x421712c4
```

Displays platform software IPv4 MFIB route processor information for the specified multicast group.

**Step 8**

```
show platform software ipv6 rp active mfib section [group-address]
```

**Example:**

```
Device# show platform software ipv6 rp active mfib section 232.1.1.1
```

```
ff3f::232:1:1:1, 2011::101:0:0:2/256 --> OBJ_INTF_LIST (0x5b)
  Obj id: 0x5b, Flags:
    OM handle: 0x421712d4
```
Displays platform software IPv6 MFIB route processor information for the specified multicast group.

**Step 9**

`show platform software mlist rp active index multicast-index-number`

**Example:**

```
Device# show platform software mlist rp active index 0x5a
```

<table>
<thead>
<tr>
<th>OCE</th>
<th>Type</th>
<th>OCE Flags</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x57</td>
<td>OBJ_ADJACENCY</td>
<td>NS, F</td>
<td>Tunnel10</td>
</tr>
<tr>
<td>0xf80000c1</td>
<td>OBJ_ADJACENCY</td>
<td>A</td>
<td>GigabitEthernet0/0/4</td>
</tr>
</tbody>
</table>

Displays platform software route processor information for the specified multicast list index.

**Step 10**

`show platform software adjacency rp active index platform-allocated-index-value`

**Example:**

```
Device# show platform software adjacency rp active index 0x57
```

Number of adjacency objects: 22

Adjacency id: 0x57 (87)
- Interface: Tunnel10, IF index: 20, Link Type: MCP_LINK_IP
- Encap Length: 30, Encap Type: MCP_ET_TUNNEL, MTU: 1470
- Flags: no-l3-inject
- Incomplete behavior type: None
- Fixup: gre
- Fixup Flags 2: pmip-udp
- Next hop addr: 33.33.33.33
- IP FRR MCP_ADJ_IPFRR_NONE 0
- OM handle: 0x4217013c

Displays platform software adjacency route processor information for the specified platform allocated index.

**Step 11**

`show ip interface brief`

**Example:**

```
Device(source gateway)# show ip interface brief
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel1</td>
<td>3.3.3.3</td>
<td>YES TFTP</td>
<td>up</td>
</tr>
<tr>
<td>....</td>
<td></td>
<td></td>
<td>up</td>
</tr>
</tbody>
</table>

The above output indicates that the relay has no connection from a gateway. The AMT relay interface will be up after it is correctly configured. If the output displays Protocol "down", you must check your configuration. If the interface command shows administratively down, you have not configured the "no shut" in the interface.

Displays errors in AMT gateway configuration.
Displaying and Verifying AMT Gateway Configuration

**SUMMARY STEPS**

1. `enable`
2. `show ip amt tunnel`
3. `show ip mroute section [group-address]`
4. `show ipv6 mroute section [group-address]`
5. `show ip mfib section [group-address]`
6. `show ipv6 mfib section [group-address]`
7. `show platform software adjacency rp active index platform-allocated-index-value`  
8. `show ip interface brief`

**DETAILED STEPS**

---

**Step 1**  
`enable`

**Example:**  
Device> enable  
Enables privileged EXEC mode.  
- Enter your password if prompted.

**Step 2**  
`show ip amt tunnel`

**Example:**  
Device(destination gateway)# show ip amt tunnel  
AMT Gateway tunnel Tunnel1:  
  Local address  UDP port  
  5.5.5.5 54358(0xD456)  
Remote address  
  3.3.3.3 2268 (0x8DC )  
Total active Relays: 1  
Device(source gateway)# show ip amt tunnel  
AMT Relay tunnel:  
  Local address  UDP port  
  3.3.3.3 2268 (0x8DC )  
Remote address  Expire time  
  5.5.5.5 54358(0xD456) 00:03:53  
Connected to 1 Gateway  
The above output is displayed if both relay and gateway is working correctly.

**Step 3**  
`show ip mroute section [group-address]`

**Example:**  
Device# show ip mroute section 232.1.1.1  
(101.0.0.2, 232.1.1.1), 2d00h/00:02:54, flags: sTI  
  Incoming interface: Tunnel10, RPF nbr 0.0.0.0, Mroute
Outgoing interface list:
GigabitEthernet0/0/4, Forward/Sparse, 2d00h/00:02:54
Displays information about the IP multicast routing (mroute) table for the specified multicast group.

**Step 4**

**show ipv6 mroute section [group-address]**

**Example:**

```
Device# show ipv6 mroute section 232.1.1.1
(2011::101:0:0:2, FF3F::232:1:1:1), 2d00h/never, flags: sTI
   Incoming interface: Tunnel10
   RPF nbr: ::
   Immediate Outgoing interface list:
      GigabitEthernet0/0/4, Forward, 2d00h/never
```
Displays information about the IPv6 mroute table for the specified multicast group.

**Step 5**

**show ip mfib section [group-address]**

**Example:**

```
Device# show ip mfib section 232.1.1.1
(101.0.0.2,232.1.1.1) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding: NA/NA/NA/NA, Other: NA/NA/NA
   Tunnel10 Flags: A
   GigabitEthernet0/0/4 Flags: F NS
   Pkts: 0/0
```
Displays the entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB) for the specified multicast group.

**Step 6**

**show ipv6 mfib section [group-address]**

**Example:**

```
Device# show ipv6 mfib section 232.1.1.1
(2011::101:0:0:2,FF3F::232:1:1:1) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding: NA/NA/NA/NA, Other: NA/NA/NA
   Tunnel10 Flags: A
   GigabitEthernet0/0/4 Flags: F NS
   Pkts: 0/0
```
Displays the entries and interfaces in the IPv6 Multicast Forwarding Information Base (MFIB) for the specified multicast group.

**Step 7**

**show platform software adjacency rp active index platform-allocated-index-value**

**Example:**

```
Device# show platform software adjacency rp active index 0x57
Number of adjacency objects: 19
   Interface: Tunnel10, IF index: 18, Link Type: MCP_LINK_IP
      Encap Length: 30, Encap Type: MCP_ET_TUNNEL, MTU: 1470
      Incomplete behavior type: None
      Fixup: gre
      Fixup Flags: 2: pmip-udp
      IP FRR MCP ADJ IFPFR_NONE 0
      OM handle: 0x4216aaaf4
```
Displays platform software adjacency route processor information for the specified platform allocated index.

**Step 8**

**show ip interface brief**
Example:
Device(destination gateway)# show ip interface brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel1</td>
<td>5.5.5.5</td>
<td>YES TFTP up</td>
<td>down</td>
</tr>
</tbody>
</table>

The Protocol: down displayed in the above output indicates that the gateway has no connection to the relay. If the interface command shows administratively down, you have not configured the "no shut" in the interface. If the command displays UNKNOWN but Protocol shows "up", then the gateway did have a connection to the relay that was terminated.

Note: It takes a few minutes before a gateway will consider a relay to be unreachable after not receiving packets from it. The gateway will then revert trying to reach the anycast address to find a new relay (in case the existing relay is down).

Displays errors in AMT gateway configuration.

Configuration Examples for Automatic Multicast Tunneling

Example: AMT Relay Configuration

The following example shows how to configure AMT relay:

```bash
enable
configure terminal
interface Tunnel10
  ip address 11.1.1.1 255.255.255.0
  no ip redirects
  ip pim sparse-mode
  ip igmp version 3
  ipv6 enable
  tunnel source Loopback0
  tunnel mode udp multipoint
  tunnel dst-port dynamic
  tunnel src-port dynamic
  amt relay traffic ip
  amt relay traffic ipv6
exit
ip multicast-routing distributed
ipv6 multicast-routing
ip pim ssm default
end
```

Example: AMT Gateway Configuration

The following example shows how to configure AMT gateway:

```bash
enable
configure terminal
interface Tunnel10
  ip address 33.1.1.1 255.255.255.0
  ip pim passive
  ip igmp version 3
  ipv6 enable
  ipv6 pim passive
  tunnel source Loopback0
  tunnel mode udp ip
```
Additional References for Automatic Multicast Tunneling

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>IP Multicast commands</td>
<td>Cisco IOS IP Multicast Command Reference</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
<tr>
<td>download documentation, software, and tools. Use these resources to install</td>
<td></td>
</tr>
<tr>
<td>and configure the software and to troubleshoot and resolve technical</td>
<td></td>
</tr>
<tr>
<td>issues with Cisco products and technologies. Access to most tools on the</td>
<td></td>
</tr>
<tr>
<td>Cisco Support and Documentation website requires a Cisco.com user ID and</td>
<td></td>
</tr>
<tr>
<td>password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature Information for Automatic Multicast Tunneling

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 Automatic Multicast Tunneling

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Multicast Tunneling</td>
<td>Cisco IOS XE Release 3.15S</td>
<td>Automatic Multicast Tunneling (AMT) provides a method to tunnel multicast data over a unicast network. The tunneling is performed between AMT relays and AMT gateways, using User Datagram Protocol (UDP) encapsulation. In Cisco IOS XE Release 3.15S, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified by this feature: <code>amt gateway traffic ip</code>, <code>amt gateway traffic ipv6</code>, <code>amt gateway relay-address</code>, <code>amt relay traffic ip</code>, <code>amt relay traffic ipv6</code>, <code>show ip amt tunnel</code>, <code>show ip amt vrf</code>, <code>show ipv mflip detail</code>, <code>show ipv6 mflip detail</code>, <code>show ip mroute detail</code>, <code>show ipv6 mroute detail</code>, <code>show platform software adjacency fp active</code>, <code>show platform software adjacency rp active</code>, <code>show platform software ip rp active mflip</code>, <code>show platform software ip fp active mflip</code>, <code>show platform software ipv6 rp active mflip</code>, <code>show platform software ipv6 fp active mflip</code>, <code>show platform software mlist</code>.</td>
</tr>
</tbody>
</table>