Implementing Multicast

- Implementing Layer-3 Multicast Routing, page 1
- Protocol Independent Multicast, page 2
- PIM-Source Specific Multicast, page 3
- Internet Group Management Protocol, page 4
- Use Case: Video Streaming, page 8

Implementing Layer-3 Multicast Routing

Multicast routing allows a host to send packets to a subset of all hosts as a group transmission rather than to a single host, as in unicast transmission, or to all hosts, as in broadcast transmission. The subset of hosts is known as group members and are identified by a single multicast group address that falls under the IP Class D address range from 224.0.0.0 through 239.255.255.255.

The multicast environment consists of senders and receivers. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message.

NCS 5500 series router supports the following protocols to implement multicast routing:

- IGMP—IGMP is used between hosts on a network (for example, LAN) and the routers on that network to track the multicast groups of which hosts are members.

- PIM SSM—Protocol Independent Multicast in Source-Specific Multicast (PIM-SSM) has the ability to report interest in receiving packets from specific source addresses (or from all but the specific source addresses), to an IP multicast address.

Prerequisites for Implementing Multicast Routing on NCS 5500 Series Router

- You must install and activate the multicast RPM package.
- You must be familiar with IPv4 multicast routing configuration tasks and concepts.
- Unicast routing must be operational.
Enabling Multicast

Configuration Example

Enables multicast routing and forwarding on all new and existing interfaces.

Router# config
Router(config)# multicast-routing
Router(config-mcast)# address-family ipv4
Router(config-mcast-default-ipv4)# interface all enable

/* In the above command, you can also indicate a specific interface (For example, interface TenGigE0/0/0/3) for enabling multicast only on that interface */
Router(config-mcast-default-ipv4)# commit

Running Configuration

Router# show running multicast routing
multicast-routing
  address-family ipv4
    interface all enable

Verification

Verify that the Interfaces are enabled for multicast.

Router# show mfib interface location 0/3/CPU0
Interface : FINT0/3/CPU0 (Enabled)
  SW Mcast pkts in : 0, SW Mcast pkts out : 0
  TTL Threshold : 0
  Ref Count : 2

  Interface : TenGigE0/3/0/0/0 (Enabled)
  SW Mcast pkts in : 0, SW Mcast pkts out : 0
  TTL Threshold : 0
  Ref Count : 3

  Interface : TenGigE0/3/0/9/0 (Enabled)
  SW Mcast pkts in : 0, SW Mcast pkts out : 0
  TTL Threshold : 0
  Ref Count : 13

  Interface : Bundle-Ether1 (Enabled)
  SW Mcast pkts in : 0, SW Mcast pkts out : 0
  TTL Threshold : 0
  Ref Count : 4

  Interface : Bundle-Ether1.1 (Enabled)
  SW Mcast pkts in : 0, SW Mcast pkts out : 0
  TTL Threshold : 0

Protocol Independent Multicast

Protocol Independent Multicast (PIM) is a multicast routing protocol used to create multicast distribution trees, which are used to forward multicast data packets.

Proper operation of multicast depends on knowing the unicast paths towards a source or an RP. PIM relies on unicast routing protocols to derive this reverse-path forwarding (RPF) information. As the name PIM implies, it functions independently of the unicast protocols being used. PIM relies on the Routing Information Base (RIB) for RPF information. Protocol Independent Multicast (PIM) is designed to send and receive multicast routing updates.

NCS 5500 series router supports Protocol Independent Multicast in Source-Specific Multicast (PIM-SSM).
PIM-Source Specific Multicast

When PIM-SM is used with SSM, multi-cast routing is easier to manage. This is because RPs (rendezvous points) are not required and therefore, no shared trees (*.G) are built.

There is no specific IETF document defining PIM-SSM. However, RFC4607 defines the overall SSM behavior. In the rest of this document, we use the term PIM-SSM to describe PIM behavior and configuration when SSM is used.

PIM in Source-Specific Multicast operation uses information found on source addresses for a multicast group provided by receivers and performs source filtering on traffic.

- By default, PIM-SSM operates in the 232.0.0.0/8 multicast group range for IPv4. To configure these values, use the `ssm range` command.
- If SSM is deployed in a network already configured for PIM-SM, only the last-hop routers must be upgraded with Cisco IOS XR Software that supports the SSM feature.
- No MSDP SA messages within the SSM range are accepted, generated, or forwarded.
- SSM can be disabled using the `ssm disable` command.
- The `ssm allow-override` command allows SSM ranges to be overridden by more specific ranges.

In many multicast deployments where the source is known, protocol-independent multicast-source-specific multicast (PIM-SSM) mapping is the obvious multicast routing protocol choice to use because of its simplicity. Typical multicast deployments that benefit from PIM-SSM consist of entertainment-type solutions like the ETTH space, or financial deployments that completely rely on static forwarding.

In SSM, delivery of data grams is based on (S,G) channels. Traffic for one (S,G) channel consists of datagrams with an IP unicast source address S and the multicast group address G as the IP destination address. Systems receive traffic by becoming members of the (S,G) channel. Signaling is not required, but receivers must subscribe or unsubscribe to (S,G) channels to receive or not receive traffic from specific sources. Channel subscription signaling uses IGMP to include mode membership reports, which are supported only in Version 3 of IGMP (IGMPv3).

To run SSM with IGMPv3, SSM must be supported on the multicast router, the host where the application is running, and the application itself. Cisco IOS XR Software allows SSM configuration for an arbitrary subset of the IP multicast address range 224.0.0.0 through 239.255.255.255.

When an SSM range is defined, existing IP multicast receiver applications do not receive any traffic when they try to use addresses in the SSM range, unless the application is modified to use explicit (S,G) channel subscription.

Benefits of PIM-SSM over PIM-SM

PIM-SSM is derived from PIM-SM. However, whereas PIM-SM allows for the data transmission of all sources sending to a particular group in response to PIM join messages, the SSM feature forwards traffic to receivers only from those sources that the receivers have explicitly joined. Because PIM joins and prunes are sent directly towards the source sending traffic, an RP and shared trees are unnecessary and are disallowed. SSM is used to optimize bandwidth utilization and deny unwanted Internet broadcast traffic. The source is provided by interested receivers through IGMPv3 membership reports.
Configuring PIM-SSM

Configuration Example

Configures SSM service for the IP address range defined by access list 4.

```
Router#config
Router(config)#ipv4 access-list 4
Router(config-ipv4-acl)#permit ipv4 any 224.2.151.0 0.0.0.255
Router(config-ipv4-acl)#exit
Router(config)#multicast-routing
Router(config-mcast)#address-family ipv4
Router(config-mcast-default-ipv4)#ssm range 4
Router(config-mcast-default-ipv4)#commit
Router(config-mcast-default-ipv4)#end
```

Running Configuration

```
Router#show running multicast-routing
multicast-routing
   address-family ipv4
      ssm range 4
      interface all enable
```

Verification

Verify if the SSM range is configured according to the set parameters:

```
Router#show access-lists 4
ipv4 access-list 4
   10 permit ipv4 any 224.2.151.0 0.0.0.255

*/Verify if the SSM is configured for 224.2.151.0/24/*:

Router#show pim group-map
IP PIM Group Mapping Table
(* indicates group mappings being used)
Group Range  Proto Client Groups RP address Info
224.0.1.39/32*  DM perm  1  0.0.0.0
224.0.1.40/32*  DM perm  1  0.0.0.0
224.0.0.0/24*  NO perm  0  0.0.0.0
224.2.151.0/24*  SSM config  0  0.0.0.0
```

Internet Group Management Protocol

Cisco IOS XR Software provides support for Internet Group Management Protocol (IGMP) over IPv4.

IGMP provides a means for hosts to indicate which multicast traffic they are interested in and for routers to control and limit the flow of multicast traffic throughout the network. Routers build state by means of IGMP messages; that is, router queries and host reports.

A set of routers and hosts that receive multicast data streams from the same source is called a multicast group. Hosts use IGMP messages to join and leave multicast groups.
IGMP messages use group addresses, which are Class D IP addresses. The high-order four bits of a Class D address are 1110. Host group addresses can be in the range 224.0.0.0 to 239.255.255.255. The address is guaranteed not to be assigned to any group. The address 224.0.0.1 is assigned to all systems on a subnet. The address 224.0.0.2 is assigned to all routers on a subnet.

NCS 5500 supports IGMPv3 by default. No configuration is required. IGMP Version 3 permits joins and leaves for certain source and group pairs instead of requesting traffic from all sources in the multicast group.

**Functioning of IGMP Routing**

The following image "IGMP Signaling", illustrates two sources, 10.0.0.1 and 10.0.1.1, that are multicasting to group 239.1.1.1.

The receiver wants to receive traffic addressed to group 239.1.1.1 from source 10.0.0.1 but not from source 10.0.1.1.

The host must send an IGMPv3 message containing a list of sources and groups (S, G) that it wants to join and a list of sources and groups (S, G) that it wants to leave. Router C can now use this information to prune traffic from Source 10.0.1.1 so that only Source 10.0.0.1 traffic is being delivered to Router C.

*Figure 1: IGMP Signaling*
Configuring IGMP Per Interface States Limit

The IGMP Per Interface States Limit sets a limit on creating OIF for the IGMP interface. When the set limit is reached, the group is not accounted against this interface but the group can exist in IGMP context for some other interface.

- If a user has configured a maximum of 20 groups and has reached the maximum number of groups, then no more groups can be created. If the user reduces the maximum number of groups to 10, the 20 joins will remain and a message of reaching the maximum is displayed. No more joins can be added until the number of groups has reached less than 10.

- If a user already has configured a maximum of 30 joins and add a max of 20, the configuration occurs displaying a message that the maximum has been reached. No state change occurs and also no more joins can occur until the threshold number of groups is brought down below the maximum number of groups.

Configuration Example

Configures all interfaces with 4000 maximum groups per interface except TenGigE interface 0/0/0/6, which is set to 3000:

```
Router#config
Router(config)#router igmp
Router(config-igmp)#maximum groups-per-interface 4000
Router(config-igmp)#interface TenGigE 0/0/0/6
Router(config-igmp-default-if)#maximum groups-per-interface 3000
Router(config-igmp-default-if)#commit
```

Running Configuration

```
router igmp
    interface TenGigE0/0/0/6
        maximum groups-per-interface 3000
    !
    maximum groups-per-interface 4000
```

Verification

```
Router#show igmp summary
Robustness Value 2
No. of Group x Interfaces 37
Maximum number of Group x Interfaces 50000
Supported Interfaces : 9
Unsupported Interfaces: 0
Enabled Interfaces : 8
Disabled Interfaces : 1
MTE tuple count : 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>No.</th>
<th>Max.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback0</td>
<td>4</td>
<td>4000</td>
</tr>
<tr>
<td>TenGigE0/0/0/0</td>
<td>5</td>
<td>4000</td>
</tr>
<tr>
<td>TenGigE0/0/0/1</td>
<td>5</td>
<td>4000</td>
</tr>
<tr>
<td>TenGigE0/0/0/2</td>
<td>0</td>
<td>4000</td>
</tr>
<tr>
<td>TenGigE0/0/0/3</td>
<td>5</td>
<td>4000</td>
</tr>
<tr>
<td>TenGigE0/0/0/6</td>
<td>5</td>
<td>3000</td>
</tr>
<tr>
<td>TenGigE0/0/0/18</td>
<td>5</td>
<td>4000</td>
</tr>
<tr>
<td>TenGigE0/0/0/19</td>
<td>5</td>
<td>4000</td>
</tr>
<tr>
<td>TenGigE0/0/0/6.1</td>
<td>3</td>
<td>4000</td>
</tr>
</tbody>
</table>
```
SSM Static Source Mapping

Configure a source (1.1.1.1) as part of a set of sources that map SSM groups described by the specified access-list (4).

**Configuration Example**

Router(config)#configure
Router(config)#ipv4 access-list 4
Router(config-ipv4-acl)#permit ipv4 any 229.1.1.0 0.0.0.255
Router(config-ipv4-acl)#exit

Router(config)#multicast-routing
Router(config-mcast)#address-family ipv4
Router(config-mcast-default-ipv4)#ssm range 4
Router(config-mcast-default-ipv4)#exit

Router(config)#router igmp
Router(config-igmp)#ssm map static 1.1.1.1 4
/*Repeat the above step as many times as you have source addresses to include in the set for SSM mapping*/
Router(config-igmp)#int te0/0/0/3
Router(config-igmp-default-if)#static-group 229.1.1.1
Router(config-igmp-default-if)#commit

**Running Configuration**

Router(config)#show run multicast-routing
multicast-routing
  address-family ipv4
    ssm range 4
      interface all enable
    !

Router(config)#show access-lists 4
ipv4 access-list 4
  10 permit ipv4 any 229.1.1.0 0.0.0.255

Router(config)#show run router igmp
router igmp
  interface TenGigE0/0/0/3
    static-group 229.1.1.1
    !
    ssm map static 1.1.1.1 4

**Verification**

Verify if the parameters are set according to the configured values:

Router(config)#show mrib route 229.1.1.1 detail
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
MoFPE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
LD - Local Disinterest, DI - Decapsulation Interface
EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface
IRMI - IR MDT Interface
(1.1.1.1,229.1.1.1) RPF nbr: 1.1.1.1 Flags: RPF
Use Case: Video Streaming

In today’s broadcast video networks, proprietary transport systems are used to deliver entire channel line-ups to each video branch office. IP based transport network would be a cost efficient/convenient alternative to deliver video services combined with the delivery of other IP based services. (Internet delivery or business services)

By its very nature, broadcast video is a service well-suited to using IP multicast as a more efficient delivery mechanism to reach end customers.

The IP multicast delivery of broadcast video is explained as follows:

1. Encoding devices in digital master headends, encode one or more video channels into a Moving Pictures Expert Group (MPEG) stream which is carried in the network via IP multicast.

2. Devices at video branch office are configured by the operator to request the desired multicast content via IGMP joins.

3. The network, using PIM-SSM as its multicast routing protocol, routes the multicast stream from the digital master headend to edge device receivers located in the video branch office. These edge devices could be edge QAM devices which modulate the MPEG stream for an RF frequency, or CMTS for DOCSIS.

Figure 2: Video Streaming