Configuring Multicast Features

This chapter provides information about configuring multicast features on the Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) line card on the Cisco 7600 series router. It includes the following topics:

- IGMP Snooping for VPLS Pseudowire on Cisco 7600 Series Ethernet Services Plus Line Cards, page 5-1
- IP and PPPoE Session Coexistence with Multicast, page 5-4
- Multicast VLAN Registration, page 5-10


Note

The information provided in this chapter is applicable to both the ES+ and ES+T line cards unless specified otherwise.

Note

On ES+ line cards, when you run the show interface command, Layer 2 multicast packets are accounted under the Broadcast category.

IGMP Snooping for VPLS Pseudowire on Cisco 7600 Series Ethernet Services Plus Line Cards

The Internet Group Management Protocol (IGMP) Snooping for VPLS Pseudowire on Cisco 7600 Series ES+ line cards provides the ability to send Layer 2 multicast frames from the customer equipment (CE) in a VPLS virtual forwarding instance (VFI) or from a multipoint bridging VLAN only to those remote peer CEs that have sent an IGMP request to join the multicast group.

IGMP Snooping for VPLS Pseudowire on Cisco 7600 Series ES+ line cards manages multicast traffic at Layer 2 by configuring the Layer 2 LAN ports dynamically to forward multicast traffic only to those ports that want to receive it. In VPLS or multipoint bridging, IGMP snooping can be set up on individual VLANs or on a VFI basis to build the membership tree, because each of the remote points of a VLAN or VFI can be identified with a virtual port and VLAN ID.
Restrictions and Usage Guidelines

When configuring the IGMP/PIM Snooping for VPLS Pseudowire on Cisco 7600 Series ES+ line cards, follow these restrictions and usage guidelines:

- IGMP snooping is enabled by default under the bridge-domain VLAN (use the `no ip igmp snooping` command to disable the default behavior).
- Globally enabling IGMP snooping enables IGMP snooping on all the existing VLAN interfaces. Globally disabling IGMP snooping disables IGMP snooping on all the existing VLAN interfaces.
- System support for 32,000 IGMP groups with no line card-specific limitation.
- Supports MultiPoint Bridging over Ethernet on Cisco 7600 Series ES+ line cards.
- Supports Virtual Private LAN Service (VPLS).
- Use the `show ip igmp snooping` privileged EXEC command to verify your IGMP settings.
- IGMP snooping works only when no tunneling operation occurs (there should not be any VLAN tags in the packet when it is put on the bridge-domain VLAN).
- During snooping, all traffic for a particular group are dropped if there are no interested receivers for that group.
- MROUTER port information should be available to all devices in the snooping domain. You can find out the MROUTER ports by:
  - Using the IP address and PIM on SVI.
  - Using the IGMP query messages heard on the segment.
  - Forcefully configuring a particular port on a switch as mrouter port using the `ip igmp snooping mrouter interface` command.
- By default, IGMP snooping is on.
- All routers acting as PE devices in a VPLS domain should have the IP address and PIM enabled on the VPLS SVI.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface vlan vlanid`
4. `no ip address ip-address mask [secondary]`
5. `ip igmp snooping`
6. `ipv6 mld snooping`
7. `xconnect vfi vfi name`
### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# enable</td>
</tr>
</tbody>
</table>
| | Enables privileged EXEC mode.  
| &bull; Enter your password if prompted. |
| **Step 2** | configure terminal |
| Example: | Router# configure terminal |
| | Enters global configuration mode. |
| **Step 3** | interface vlan vlanid |
| Example: | Router(config)# interface vlan 12 |
| | Creates a unique VLAN ID number and enters subinterface configuration mode. |
| **Step 4** | no ip address ip-address mask [secondary] |
| Example: | Router(config)# no ip address |
| | Disables IP processing and enters interface configuration mode. |
| **Step 5** | ip igmp snooping |
| Example: | Router(config-if)# ip igmp snooping |
| | Enables IGMP snooping. To disable IGMP snooping, use the no form of this command. |
| **Step 6** | ipv6 mld snooping |
| Example: | Router(config)# ipv6 mld snooping |
| | Enables Multicast Listener Discovery version 2 (MLDv2) snooping globally. To disable the MLDv2 snooping globally, use the no form of this command. |
| **Step 7** | xconnect vfi vfi name |
| Example: | Router(config-if)# xconnect vfi vfi16 |
| | Specifies the Layer 2 VFI that you are binding to the VLAN port. |

### Example

This is a VLAN configuration.

```
Router# enable
Router# configure terminal
Router(config)# interface Vlan700
Router(config)# no ip address
Router(config-if)# ip igmp snooping
Router(config-if)# ipv6 mld snooping
Router(config-if)# xconnect vfi vfi16
```

### Verification

Use the `show ip igmp interface vlan` command to verify a configuration.
IP and PPPoE Session Coexistence with Multicast

The IP and PPPoE Session Coexistence with Multicast feature allows you to converge IP subscribers and multicast users on the same VLAN. IP subscriber sessions are supported on non-access type subinterfaces through which multicast control and data traffic can pass through whether the IP session is absent or present.

The IP and PPPoE Session Coexistence with Multicast feature does not support IP Interface session and PPP session types. When multicast traffic is received by interfaces hosting IP Interface or PPP sessions, the multicast traffic will be treated as part of the session traffic.

- Multicast traffic streams towards the access node (downstream direction) co-exist on the interface that is configured for Sessions (IP or PPPoEoX).
  - This is not for per session multicast but allows multicast stream to co-exist on the interfaces on which hosts sessions exist.
  - The multicast stream is targeted for an Access-Node (DSLAM/switch) that handles per subscriber replication.

Additionally, QoS priority queueing-2 and policing for multicast traffic is supported.

- From QoS treatment perspective:
  - Multicast traffic shaping is not required at subinterface (Dot1Q/QinQ) level.
  - Multicast traffic need to be considered as PQ2 traffic (at port level) on the egress side.
- Multicast traffic co-existence is required only for Ethernet main and subinterfaces.
- Support for IP Multicast co-existence on ISG aware sub-interfaces is HA/SSO capable.

Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines when configuring QoS with the IP and PPPoE Session Coexistence with Multicast:

- All multicast traffic on a non-access subscriber interface will be treated as priority level2 packets.
- Use the `platform subscriber-multicast priority-level2 police` command to configure the percentage rate of port bandwidth that the multicast traffic will be policed at.
- The percentage rate configured will be applicable on a per port basis.
- When configured, all multicast traffic on non-access subscriber interface will be treated as priority level 2 and policed at the configured percent of the individual ports bandwidth.
- When not configured, multicast traffic is not treated as priority level2 traffic.
- The IP and PPPoE Session Coexistence with Multicast feature is not supported on sub-interfaces created with `access` keyword option.
- Maximum number of IP and PPPoE subscriber sessions supported per port group is 4000.
- Maximum number of IP and PPPoE subscriber sessions supported per line card is 16000.
Configuring IP and PPPoE Session Coexistence with Multicast

Summary Steps

1. enable
2. configure terminal
3. ip multicast-routing [vrf vrf-name] [distributed]
4. ip pim rp-address ip-address [group-access-list-number] [override]
5. interface gigabitethernet slot/port or interface tengigabitethernet slot/port
6. encapsulation dot1q vlan-id
7. [no] ip address
8. [no] ip pim {sparse-mode | sparse-dense-mode | dense-mode [proxy-register {list access-list | route-map map-name}]}
9. ip subscriber routed
10. initiator {dhcp [class-aware] | static | nclassified ip-address}
11. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ip multicast-routing</td>
<td>Enables IP multicast routing.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# ip multicast-routing</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>ip pim rp-address ip-address [group-access-list-number] [override]</td>
<td>Configures the IP address of a PIM rendezvous point (RP) for a particular group access list.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# ip pim rp-address 198.92.37.33</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>interface gigabitethernet slot/port</td>
<td>Specifies the Gigabit Ethernet interface to configure, where:</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface gigabitethernet 4/1</td>
<td></td>
</tr>
</tbody>
</table>
## IP and PPPoE Session Coexistence with Multicast

### Step 6

**Command:**

```plaintext
encapsulation dot1q vlan-id {cos | comma | hyphen | etype}
```

**Example:**

Router(config-if-srv)# encapsulation dot1q 100?

**Purpose:** Defines the matching criteria to map dot1Q ingress frames on an interface to the appropriate service instance. VLAN ID is an integer in the range 1 to 4094. Hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs. Available options are CoS and ethertype.

### Step 7

**Command:**

```plaintext
[no] ip address
```

**Example:**

Router(config-if)# no ip address

**Purpose:** Assigns an IP address and subnet mask to the EtherChannel.

### Step 8

**Command:**

```plaintext
no ip pim {sparse-mode | sparse-dense-mode | dense-mode [proxy-register {list access-list | route-map map-name}]}
```

**Example:**

Router(config-if)# ip pim sparse-mode

**Purpose:** Enables Protocol Independent Multicast (PIM) on an interface.

### Step 9

**Command:**

```plaintext
ip subscriber routed
```

**Example:**

Router(config-if)# ip subscriber routed

**Purpose:** Specifies the type of IP subscriber to be hosted on the interface, and enters ISG IP subscriber configuration mode.

### Step 10

**Command:**

```plaintext
initiator {dhcp [class-aware] | static | unclassified ip-address}
```

**Example:**

Router(config-if)# ip pim sparse-mode

**Purpose:** Configures ISG to create an IP subscriber session upon receipt of the specified packet type.

- **dhcp**—ISG will initiate an IP session upon receipt of a DHCP DISCOVER packet. The class-aware keyword allows ISG to influence the IP address assigned by DHCP by providing DHCP with a class name.
- **radius-proxy**—ISG will initiate an IP session upon receipt of a RADIUS Access-Request packet.
- **unclassified ip-address**—ISG will initiate an IP session upon receipt of the first IP packet with an unclassified IP source address.
- This command can be entered more than once to specify more than one method of IP session initiation.

### Step 11

**Command:**

```plaintext
end
```

**Example:**

Router(config-if)# end

**Purpose:** Ends the current configuration session.
## Configuring a PQ2 Policer Under the Main Interface

### Summary Steps

1. `enable`
2. `configure terminal`
3. `interface gigabitethernet slot/port` or `interface tengigabitethernet slot/port`
4. `encapsulation dot1q vlan-id`
5. `[no] ip address`
6. `load-interval seconds`
7. `platform subscriber-multicast priority-level2 police rate_in_kbps`
8. `end`

### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `enable` | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Example:** | `Router> enable` |  |
| **Step 2** | `configure terminal` | Enters global configuration mode. |
| **Example:** | `Router# configure terminal` |  |
| **Step 3** | `interface gigabitethernet slot/port` | Specifies the Gigabit Ethernet interface to configure, where:  
- `slot/port`—Specifies the location of the interface. |
| **Example:** | `Router(config)# interface gigabitethernet 4/1` | Creates the port-channel interface. |
| **Step 4** | `encapsulation dot1q vlan-id {cos | comma | hyphen | ethtype}` | Defines the matching criteria to map dot1Q ingress frames on an interface to the appropriate service instance. VLAN ID is an integer in the range 1 to 4094. Hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs. Available options are CoS and ethertype. |
| **Example:** | `Router(config-if-srv)# encapsulation dot1q 100?` |  |
| **Step 5** | `[no] ip address` | Assigns an IP address and subnet mask to the EtherChannel. |
| **Example:** | `Router(config-if)# no ip address` |  |
### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td>load-interval seconds</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# load-interval 30</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>platform subscriber-multicast priority-level2 police rate in kbps</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# platform subscriber-multicast priority-level2 police 200</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# end</td>
</tr>
</tbody>
</table>

#### Note

This command is applicable to multicast traffic being sent on the main or subinterfaces that are configured with `ip subscriber` command or `pppoe enable` command. Multicast traffic on other interfaces on the same port are not impacted by this command. In case of port-channel interfaces, the command should be configured on the member interfaces of the port-channel.

#### Examples

This is an example of how to configure a nonaccess subinterface for multicast and ISG sessions:

```
ip multicast-routing
ip pim rp-address 192.10.10.1
interface GigabitEthernet4/13.200
  encapsulation dot1Q 200
  ip address 192.10.10.1 255.255.255.0
  ip pim sparse-mode
  ip subscriber routed
  initiator unclassified ip-address
end
```

This is an example of how to configure PQ2 policer under main interface:

```
interface GigabitEthernet4/13
  ip address 33.0.0.1 255.0.0.0
  load-interval 30
  platform subscriber-multicast priority-level2 police 200
end
```

#### Verification

Use the following commands to verify operation.
Troubleshooting

This section describes how to troubleshoot common Multicast issues.

<table>
<thead>
<tr>
<th>Scenarios/Problems</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>How do I know the multicast groups with receivers that are directly connected to</td>
<td>Use the <strong>show ip igmp groups</strong> command. This is a sample output of the</td>
</tr>
<tr>
<td>the router and that were learned through IGMP?</td>
<td>command: Router# show ip igmp groups</td>
</tr>
<tr>
<td></td>
<td>IGMP Connected Group Membership</td>
</tr>
<tr>
<td></td>
<td>Group Address</td>
</tr>
<tr>
<td></td>
<td>Reporter</td>
</tr>
<tr>
<td></td>
<td>239.255.255.254</td>
</tr>
<tr>
<td></td>
<td>172.21.200.159</td>
</tr>
<tr>
<td></td>
<td>172.21.200.1</td>
</tr>
<tr>
<td></td>
<td>172.16.214.251</td>
</tr>
<tr>
<td></td>
<td>172.21.200.11</td>
</tr>
<tr>
<td></td>
<td>224.0.1.40</td>
</tr>
<tr>
<td></td>
<td>172.21.200.155</td>
</tr>
<tr>
<td></td>
<td>172.21.200.206</td>
</tr>
<tr>
<td></td>
<td>232.1.1.1</td>
</tr>
<tr>
<td></td>
<td>172.21.200.206</td>
</tr>
</tbody>
</table>

| How do I verify information about the multicast MAC address table entries?        | Use the **show mac-address-table multicast** command. This example shows   |
|                                                                                  | how to display information about the MAC address table for MLDv2 snooping: |
|                                                                                  | Router# show mac-address-table multicast mld-snooping                       |
|                                                                                  | vlan mac address type learn qos ports                                     |
|                                                                                  | --+------------+-------------------+-------------------+-------------------+-------------------+|
|                                                                                  | | mac address type | learn | qos | ports |
|                                                                                  | ---+---------------+--------+-----+---+-------------------------------|
|                                                                                  | --- 3333.0000.0001 static | Yes - Switch,Stby-Switch |
|                                                                                  | --- 3333.0000.000d static | Yes - Fa2/1,Fa4/1,Router,Switch |
|                                                                                  | --- 3333.0000.0016 static | Yes - Switch,Stby-Switch |

| How do I display information about PIM neighbors discovered by PIMv1 router query | Use the **show ip pim neighbor** command. This is a sample output of the   |
| messages or PIMv2 hello messages?                                                | command: Router# show ip pim neighbor                                        |
|                                                                                  | PIM Neighbor Table                                                           |
|                                                                                  | Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,    |
|                                                                                  | S - State Refresh Capable                                                    |
|                                                                                  | Neighbor | Interface | Uptime/Expires | Ver | DR |
|                                                                                  | Address | Prio/Mode |              |     |    |
|                                                                                  | 10.0.0.1 | S         | 00:01:29/00:01:15 v2 | 1/  |
|                                                                                  | 10.0.0.3 | DR S P    | 00:01:15/00:01:28 v2 | 1/  |
Multicast VLAN Registration

Multicast VLAN Registration (MVR) is used to deploy multicast traffic across an Ethernet ring-based service-provider network. For example, the broadcast of multiple television channels over a service-provider network.

MVR performs the following:

- Identifies the MVR IP multicast streams and their associated IP multicast groups in the Layer 2 forwarding table.
• Intercepts the IGMP messages.
• Allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the multicast VLAN.
• Allows a single multicast VLAN to be shared in the network while subscribers remain in separate VLANs.
• Provides the ability to continuously send multicast streams in the multicast VLAN and isolate the streams from the subscriber VLANs for bandwidth and security reasons.
• Modifies the Layer 2 forwarding table to include or remove the subscriber as a receiver of the multicast stream, even though the receivers might be in a different VLAN from the source. This forwarding behavior selectively allows traffic to cross between different VLANs.

The router forwards multicast data for MVR IP multicast streams only to MVR ports on which hosts have joined, either by IGMP reports or by MVR static configuration. The router forwards IGMP reports received from MVR hosts only to the source (uplink) port. This eliminates using unnecessary bandwidth on MVR data port links.

**Note**

Only layer 2 ports participate in MVR. You must configure ports as MVR receiver ports. Only one MVR multicast VLAN per router is allowed.

During MVR, subscriber ports subscribe and unsubscribe multicast streams by sending out IGMP join and leave messages. These messages can originate from an IGMP version-2-compatible host with an Ethernet connection. Although MVR operates on the underlying mechanism of IGMP snooping, the two features operate independent of each other. However, if IGMP snooping and MVR are both enabled, MVR reacts only to join and leave messages from multicast groups configured under MVR. Join and leave messages from all other multicast groups are managed by IGMP snooping.

**Using MVR in a Multicast Television Application**

In a multicast television application, a PC or a television with a set-top box receives the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. Figure 5-1 illustrates this configuration.

The MVR feature in a multicast television application functions in this sequence:

• DHCP assigns an IP address to the set-top box or the PC. When a subscriber selects a channel, the set-top box or PC sends an IGMP report to Switch A to join the appropriate multicast. If the IGMP report matches one of the configured IP multicast group addresses, the Source Port (SP) CPU modifies the hardware address table to include this receiver port and VLAN as a forwarding destination of the specified multicast stream when it is received from the multicast VLAN. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.
When a subscriber changes channels or switches off the television, the set-top box sends an IGMP leave message to the multicast stream. The SP CPU sends a MAC-based general query through the receiver port VLAN. If there is another set-top box in the VLAN still subscribing to this group, that set-top box must respond within the maximum response time specified in the query. If the CPU does not receive a response, it eliminates the receiver port as a forwarding destination for this group.

Unless the Immediate Leave feature is enabled, when the router receives an IGMP leave message from a subscriber on a receiver port, it sends out an IGMP query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership. With the Immediate Leave feature enabled, an IGMP query is not sent from the receiver port on which the IGMP leave was received. As soon as the leave message is received, the receiver port is removed from multicast group membership, which speeds up leave latency. Enable the Immediate Leave feature only on receiver ports to which a single receiver device is connected.

MVR eliminates the need to duplicate television-channel multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is only sent around the VLAN trunk once—only on the multicast VLAN. The IGMP leave and join messages are in the VLAN to which the subscriber port...
is assigned. These messages dynamically register for streams of multicast traffic in the multicast VLAN on the layer 3 device, Switch B. The access layer switch, Switch A, modifies the forwarding behavior to allow the traffic to be forwarded from the multicast VLAN to the subscriber port in a different VLAN, selectively allowing traffic to cross between two VLANs.

- IGMP reports are sent to the same IP multicast group address as the multicast data. The Switch A CPU must capture all IGMP join and leave messages from receiver ports and forward them to the multicast VLAN of the source (uplink) port.

## Configuring MVR

For information on configuring and troubleshooting the MVR, see:
