IGMP Explicit Tracking

This module describes the explicit tracking of hosts, groups, and channels for the Internet Group Management Protocol (IGMP).

IGMP Explicit Tracking

This module describes the explicit tracking of hosts, groups, and channels for the Internet Group Management Protocol (IGMP).

Restrictions for IGMP Explicit Tracking

The following restrictions apply to this feature.

- If one or more hosts that supports only IGMP Version 1 or Version 2 are present on a network, the leave latencies for the multicast groups to which these hosts are joined will revert to the leave latencies of the IGMP version of the hosts—approximately 3 seconds for IGMP Version 2 and up to 180 seconds for IGMP Version 1. This condition affects only multicast groups to which these legacy hosts are actually joined at any given point in time. In addition, the membership reports for these multicast groups sent by IGMPv3 hosts may revert to IGMP Version 1 or Version 2 membership reports, thus disabling explicit tracking of those host memberships.
- Explicit tracking of IGMP Version 3 lite (IGMP v3lite) or URL Rendezvous Directory (URD) channel membership reports is not supported. Therefore, the leave latency for multicast groups sending traffic to hosts using IGMPv3 lite or URD will be determined by the leave latency of the version of IGMP configured on the hosts (for IGMPv3, the leave latency is typically 3 seconds when explicit tracking is not configured).

Information About IGMP Explicit Tracking

IGMP Explicit Tracking

The Internet Group Management Protocol (IGMP) is used by IP hosts to report their multicast group memberships to neighboring multicast devices. The IGMP Explicit Tracking feature enables a multicast device to explicitly track the membership of all multicast hosts in a particular multiaccess network. IGMP explicit tracking can be enabled globally and on Layer3 interfaces.

The explicit tracking of hosts, groups, and channels enables the device to keep track of each individual host that is joined to a particular group or channel. The main benefits of this feature are that it provides minimal leave latencies, faster channel changing, and improved diagnostics capabilities for IGMP.

Minimal Leave Latencies

The main benefit of the explicit tracking of hosts, groups, and channels in IGMP is to allow minimal leave latencies when a host leaves a multicast group or channel. The length of time between a host wanting to leave and a device stopping traffic forwarding is called the IGMP leave latency. A device configured with IGMP Version 3 (IGMPv3) and explicit tracking can immediately stop forwarding traffic if the last host to request to receive traffic from the device indicates that it no longer wants to receive traffic. The leave latency is thus bound only by the packet transmission latencies in the multiaccess network and the processing time in the device.

In IGMP Version 2, when a device receives an IGMP leave message from a host, it must first send an IGMP group-specific query to learn if other hosts on the same multiaccess network are still requesting to receive traffic. If after a specific time (the default value is approximately 3 seconds) no host replies to the query, the device will then stop forwarding the traffic. This query process is required because, in IGMP Version 1 and 2, IGMP membership reports are suppressed if the same report is already sent by another host in the network. Therefore, it is impossible for the device to reliably know how many hosts on a multiaccess network are requesting to receive traffic.

Faster Channel Changing

In networks where bandwidth is constrained between multicast devices and hosts (like in xDSL deployments), the bandwidth between devices and hosts is typically large enough to only sustain, in general, N multicast streams to be received in parallel. In these deployments, each host will typically join to only one multicast stream and the overall number of allowed hosts will be limited to N. The effective leave latency in these environments defines the channel change time of the receiver application—a single host cannot receive the new multicast stream before forwarding of the old stream has stopped. If an application tries to change the channel faster than the leave latency, the application will overload the bandwidth of the access network, resulting in a temporary degradation of traffic flow for all hosts. The explicit tracking of hosts, groups, and channels in IGMP allows for minimal leave latencies, and thus allows for fast channel changing capabilities.

Improved Diagnostic Capabilities

The explicit tracking of hosts, groups, and channels in IGMP allows network administrators to easily determine which multicast hosts are joined to other multicast groups or channels.

How to Configure IGMP Explicit Tracking

Enabling Explicit Tracking Globally

You can enable explicit-tracking globally and on Layer 3 interfaces.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip igmp snooping vlan** *vlan-id* **explicit-tracking** **Example:** `Device(config)# ip igmp snooping vlan 1 explicit-tracking`	Enables IGMP explicit host tracking.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Enabling Explicit Tracking on Layer 3 Interfaces

You can enable explicit-tracking globally and on Layer 3 interfaces.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface vlan 77`	Configures an interface and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 10.1.1.1 255.255.255.254`	Sets a primary or secondary IP address for an interface.
Step 5	**ip pim sparse-mode** **Example:** `Device(config-if)# ip pim sparse-mode`	Enables Protocol Independent Multicast (PIM) sparse mode on an interface.

	Command or Action	Purpose
Step 6	**ip igmp version 3** **Example:** `Device(config-if)# ip igmp version 3`	Configure Internet Group Management Protocol (IGMP) Version 3 (IGMPv3) on the device.
Step 7	**ip igmp explicit-tracking** **Example:** `Device(config-if)# ip igmp explicit-tracking`	Enables IGMP explicit host tracking.
Step 8	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuration Examples for IGMP Explicit Tracking

Example: Enabling Explicit Tracking

The following example shows a basic configuration to enable IGMP explicit tracking globally:

```
Device# configure terminal
Device(config)# ip multicast routing
Device(config)# ip igmp snooping vlan 1 explicit-tracking
Device(config)# end
```

The following example shows a basic configuration to enable IGMP explicit tracking on Layer 3 interfaces:

```
Device# configure terminal
Device(config)# interface vlan 77
Device(config-if)# ip address 10.1.1.1 255.255.255.254
Device(config-if)# ip pim sparse-mode
Device(config-if)# ip igmp version 3
Device(config-if)# ip igmp explicit-tracking
Device(config-if)# end
```

Displaying IGMP Explicit Tracking Information

To display host membership information, perform this task:

Procedure

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **show ip igmp snooping membership** [**interface** *interface_num*] [**vlan** *vlan-id*] [**reporter** *a.b.c.d*] [**source** *a.b.c.d* **group** *a.b.c.d*]

Example:

```
Device# show ip igmp snooping membership vlan 20
```

Displays Explicit Host Tracking (EHT) information. This command is valid only if EHT is enabled on the switch.

Note By default, EHT can have a maximum of 128K entries in the EHT database. However, we recommend not to have more than 4000 entries, to avoid performance issues.

With the EHT feature enabled, the entries that are updated in the IGMP Snooping Membership table do not age out. Use the **clear ip igmp snooping membership vlan** command to clear the entries from the explicit host tracking table.

Example

The following example shows how to display host membership information for VLAN 100 and to delete the EHT database:

```
Device# show ip igmp snooping membership vlan 100
Snooping Membership Summary for Vlan 100
----------------------------------------
Total number of channels: 2
Total number of hosts   : 1

Source/Group     Interface Reporter      Vlan Uptime   Last-Join/Last-Leave
-------------------------------------------------------------------------
0.0.0.0/228.1.1.1 Po9       99.99.1.2    100  00:00:00 00:00:01/00:00:01
0.0.0.0/228.1.1.2 Po9       99.99.1.2    100  00:00:00 00:00:01/00:00:01

Device# clear ip igmp snooping membership vlan 100
```

Verifying IGMP Explicit Tracking

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ip igmp snooping vlan** *vlan-ID*

Example:

```
Device# show ip igmp snooping vlan 77
```

Displays snooping information in a Catalyst VLAN.

```
Device# show  ip igmp  snooping vlan  77

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping              : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 77:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Explicit host tracking               : Enabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
Device#
```

Step 3 **show ip igmp groups** *interface-type interface-number*

Example:

```
Device# show ip igmp groups GigabitEthernet 1/0/24
```

Displays the multicast groups that are directly connected to a device, and that are learned through IGMP.

```
show ip igmp groups GigabitEthernet 1/0/24

IGMP Connected Group Membership
Group Address    Interface               Uptime    Expires   Last Reporter   Group Accounted
203.0.113.245    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.244    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.247    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.246    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.241    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.240    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.243    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.242    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.253    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.252    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.221    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.254    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.249    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.248    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.251    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.250    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.228    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.229    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
203.0.113.230    GigabitEthernet1/0/24     00:00:35  stopped   10.34.34.2
```

```
203.0.113.231    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.224    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
```

Step 4 **show ip igmp membership tracked**

Example:

```
Device# show ip igmp membership tracked
```

Displays the multicast groups with the explicit tracking feature enabled.

```
Device# show ip igmp  membership tracked

Flags: A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, U - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP, the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (G))
Reporter:
       <mac-or-ip-address> - last reporter if group is not explicitly tracked
       <n>/<m>      - <n> reporter in include mode, <m> reporter in exclude

 Channel/Group                  Reporter        Uptime   Exp.  Flags  Interface
 *,203.0.113.10                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.10        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.11                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.11        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.14                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.14        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.15                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.15        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.12                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.12        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.13                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.13        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.19                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.19        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.18                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.18        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.17                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.17        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.16                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.16        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.40                  0/1             00:20:48 02:16 3LAT   Gi1/0/24
 *,209.165.201.1                 10.34.34.1      00:20:48 02:16 3LT    Gi1/0/24
Device#
```

Step 5 **show ip igmp snooping vlan** *vlan-ID*

Example:

```
Device# show ip igmp snooping vlan 77
```

Displays the IGMP snooping configuration on a VLAN.

```
Device# show  ip igmp  snooping vlan  77

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping              : Enabled
```

```
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 77:
--------
IGMP snooping                          : Enabled
IGMPv2 immediate leave                 : Disabled
Explicit host tracking                 : Enabled
Multicast router learning mode         : pim-dvmrp
CGMP interoperability mode             : IGMP_ONLY
Robustness variable                    : 2
Last member query count                : 2
Last member query interval             : 1000
Device#
```

Feature History for IGMP Explicit Tracking

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 IGMP Explicit Tracking

Feature Name	Release	Feature Information
IGMP Explicit Tracking	Cisco IOS XE Everest 16.6.1	This module describes the explicit tracking of hosts, groups, and channels for IGMP. In Cisco IOS XE Everest 16.6.1, this feature was implemented on the following platforms: • Cisco Catalyst 3850 Series Switches