Mroute Limit and IGMP Limit

Feature history for mroute limit and IGMP limit

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature name and description	Supported platform
Cisco IOS XE 17.18.1	Mroute limit: The Multicast Route Limit feature allows global and per MVRF state limiters configuration, which impose limits on the number of mroutes that can be added to the global table or to a particular MVRF table. IGMP limit: The IGMP State Limit feature allows IGMP state limiters configuration, which impose limits on mroute states resulting from IGMP membership reports.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Understand mroute limit and IGMP limit

The Multicast Route Limit feature allows global and per MVRF state limiters configuration, which impose limits on the number of multicast routes (mroutes) that can be added to the global table or to a particular Multicast Virtual Routing and Forwarding (MVRF) table.

The IGMP State Limit feature allows IGMP state limiters configuration, which impose limits on mroute states resulting from Internet Group Management Protocol (IGMP) membership reports (IGMP joins).

Mroute state limit

Multicast route state limit refers to a limit on the number of multicast routing entries (mroute states) that a device can maintain. This limit helps prevent control plane overload by restricting the number of multicast routes the device processess and stores, ensuring stable and fair resource usage. In Multi-VRF (MVRF) environments, the MVRF mroute state limit allows administrators to set multicast route limits individually for each VRF.

Global mroute state limiters limit the number of mroutes added to the global table on a device. Configuring a global mroute state limiter protects a device in a multicast DoS attack by preventing mroutes from overrunning the device.

Per VRF mroute state limiters limit the number of mroutes added to an MVRF table. Use per MVRF mroute state limits to ensure fair sharing of mroutes between different MVRFs.

Mroute state limit feature design

Global and per MVRF mroute state limiters are configured using the **ip multicast route-limit** command in global configuration mode. This command imposes limits on the number of mroutes that can be added to the global table or to a particular MVRF table, respectively.

The syntax of the **ip multicast route-limit** command is as follows:

ip multicast [**vrf** *vrf-name*] **route-limit** *limit* [*threshold*]

Issuing the **ip multicast route-limit** command without the optional **vrf** keyword and *vrf-name* arguments configures a global mroute state limiter. The optional **vrf** keyword and *vrf-name* arguments are used with the **ip multicast limit** command to configure per MVRF mroute state limiters.

The value specified for the required *limit* argument defines the maximum number of mroutes that can be added to either the global table or a particular MVRF table, respectively.

In addition, for both global and per MVRF mroute state limiters, the optional *threshold* argument is available to set mroute threshold limits.

Note

- When configuring global and per VRF mroute state limiters, you can only configure one limit for the global table and one limit per MVRF table.
- Global and per MVRF mroute state limiters operate independently. They can be used either alone or together, depending on the admission control requirements of your network.

Mechanics of mroute state limiters

Here is how global and per MVRF mroute state limiters work:

- When an mroute state is created on a device, the Cisco IOS software checks if the global or per MVRF mroute state limiter's limit has been reached.

- States for mroutes that exceed the configured limit for the global or the per MVRF mroute state limiter are not created on the device, and a warning message in this format is generated:

```
% MROUTE-4-ROUTELIMIT : <current mroute count> exceeded multicast route-limit of <mroute
 limit value>
```

- When an mroute threshold limit is also configured for the global or the per MVRF mroute state limiter, each time the state for an mroute is created on a device, the Cisco IOS software also checks to see if the mroute threshold limit has been reached. If the mroute threshold limit is exceeded, a warning message in this format is generated:

```
% MROUTE-4-ROUTELIMITWARNING : multicast route-limit warning <current mroute count>
threshold <mroute threshold value>
```

  Warning messages continue until the number of mroutes exceeds the configured limit or falls below the mroute threshold.

IGMP state limit

The IGMP State Limit feature allows the configuration of IGMP state limiters to impose limits on mroute states resulting from IGMP membership reports (IGMP joins), applicable globally or on a per-interface basis. Membership reports that exceed the configured limits are excluded from the IGMP cache. You can use the IGMP State Limit feature to prevent DoS attacks and enable a multicast CAC mechanism in network environments where multicast flows utilize similar bandwidth.

Note IGMP state limiters impose limits on the number of mroute states resulting from IGMP, IGMP v3lite, and URL Rendezvous Directory (URD) membership reports on a global or per interface basis.

IGMP state limit feature design

- In global configuration mode, configure IGMP state limiters to set a device-wide limit on cached IGMP membership reports.
- In interface configuration mode, configure IGMP state limiters to limit the number of IGMP membership reports per interface.
- Use ACLs to exclude certain groups or channels from being counted against the interface limit. A standard or an extended ACL can be specified. Standard ACL usage: Define the (*, G) state to be excluded from an interface's limit. Extended ACL usage: Define the (S, G) state excluded from the interface limit. An extended ACL also can be used to define the (*, G) state to be excluded from the limit on an interface, by specifying 0.0.0.0 for the source address and source wildcard--referred to as (0, G)--in the permit or deny statements that compose the extended access list.
- You can only configure one global limit per device and one limit per interface.

Mechanics of IGMP state limiters

The mechanics of IGMP state limiters are as follows:

- When a device receives an IGMP membership report for a group or channel, the Cisco IOS software determines whether the limit for either the global IGMP state limiter or the per interface IGMP state limiter is reached.
- IGMP membership reports are honored if only a global IGMP state limiter is configured and its limit has not been reached. When the configured limit is reached, subsequent IGMP membership reports are ignored, and a warning message is generated in these formats:

```
%IGMP-6-IGMP_GROUP_LIMIT: IGMP limit exceeded for <group (*, group address)> on <interface
 type number> by host <ip address>
```

```
%IGMP-6-IGMP_CHANNEL_LIMIT: IGMP limit exceeded for <channel (source address, group
address)> on <interface type number> by host <ip address>
```

- If only per interface IGMP state limiters are configured, then each limit is only counted against the interface on which it was configured.
- If both a global IGMP state limiter and per interface IGMP state limiters are configured, the limits configured for the per interface IGMP state limiters are still enforced but are constrained by the global limit.

Prerequisites for mroute limit and IGMP limit

- Ensure IP multicast is enabled and configure the Protocol Independent Multicast (PIM) interfaces.
- Configure MVRFs on the PE device before configuring per MVRF mroute state limiters.

Configure mroute limit and IGMP limit

This section provides configuration information about mroute limit and IGMP limit.

Configure a global mroute state limiter

Perform this task to limit the number of mroutes that can be added to the global table. States for mroutes that exceed the global mroute limit will not be created.

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.

	Command or Action	Purpose
Step 3	**ip multicast route-limit** *limit* [*threshold*] **Example:** `Device(config)# ip multicast route-limit 1500 1460`	Limits the number of mroutes that can be added to the global table. • For the required *limit* argument, specify the limit on the number of mroutes that can be added to the global table. The range is from 1 to 2147483647. • Use the optional *threshold*argument to set an mroute threshold limit. The range is from 1 to 2147483647.
Step 4	**end** **Example:** `Device(config)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 5	**show ip mroute count** **Example:** `Device# show ip mroute count`	(Optional) Displays mroute data and packet count statistics. • Use this command to verify the number of mroutes in the global table.

Configure per MVRF mroute state limiters

Perform this optional task to configure per MVRF mroute state limiters, limiting the number of mroutes added to a specific MVRF table.

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	**ip multicast vrf** *vrf-name* **route-limit** *limit* [*threshold*] **Example:** `Device(config)# ip multicast vrf red route-limit 1500 1460`	Limits the number of mroutes that can be added to a particular MVRF table. • For the **vrf** keyword and *vrf-name* argument, specify the MVRF for which to apply the limit.

	Command or Action	Purpose
		• For the required *limit* argument, specify the limit on the number of mroutes that can be added to the MVRF table (for the specified MVRF). The range is from 1 to 2147483647. • Use the optional *threshold* argument to set an mroute threshold limit. The range is from 1 to 2147483647.
Step 4	**end** **Example:** `Device(config)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 5	**show ip mroute vrf** *vrf-name* **count** **Example:** `Device# show ip mroute vrf red count`	(Optional) Displays mroute data and packet count statistics related to the specified MVRF. • Use this command to verify the number of mroutes in a particular MVRF table.

Configure global IGMP state limiters

Perform this optional task to configure one global IGMP state limiter per device.

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	**ip igmp limit** *number* **Example:** `Device(config)# ip igmp limit 150`	Configures a global limit on the number of mroute states resulting from IGMP membership reports (IGMP joins).
Step 4	**end** **Example:**	Ends the current configuration session and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-if)# end`	
Step 5	**show ip igmp groups** **Example:** `Device# show ip igmp groups`	(Optional) Displays the multicast groups with receivers that are directly connected to the device and that were learned through IGMP.

Configure per interface IGMP state limiters

Perform this optional task to configure a per interface IGMP state limiter.

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 GigabitEthernet 1/0/0`	Enters interface configuration mode. • Specify an interface that is connected to hosts.
Step 4	**ip igmp limit** *number* [**except** *access-list*] **Example:** `Device(config-if)# ip igmp limit 100`	Configures a per interface limit on the number of mroutes states created as a result of IGMP membership reports (IGMP joins).

Step 5	Do one of these:
	• **exit**
	• **end**
	Example:
	`Device(config-if)# exit`
	`Device(config-if)# end`
		• (Optional) Ends the current configuration session and returns to global configuration mode. Repeat steps 3 and 4 to configure a per interface limiter on another interface.
		• Ends the current configuration session and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show ip igmp interface** [*type number*] **Example:** `Device# show ip igmp interface`	(Optional) Displays information about the status and configuration of IGMP and multicast routing on interfaces.
Step 7	**show ip igmp groups** **Example:** `Device# show ip igmp groups`	(Optional) Displays the multicast groups with receivers that are directly connected to the device and that were learned through IGMP.

Configuration examples

Refer this section for configuration examples of mroute limit and IGMP limit.

Example: Configure mroute state limiters

This example shows how to configure a global mroute state limiter. In this example, a global mroute state limiter is configured with an mroute limit of 1500 and an mroute threshold limit of 1460.

```
ip multicast route-limit 1500 1460
```

This is a sample mroute threshold warning message. The output shows that the configured mroute threshold limit of 1460 has been exceeded by one mroute.

```
%MROUTE-4-ROUTELIMITWARNING : multicast route-limit warning 1461 threshold 1460
```

This is a sample mroute exceeded warning message. The output shows that the configured mroute limit of 1500 has been exceeded by one mroute. The device does not create states for mroutes that exceed the configured limit of the global mroute state limiter.

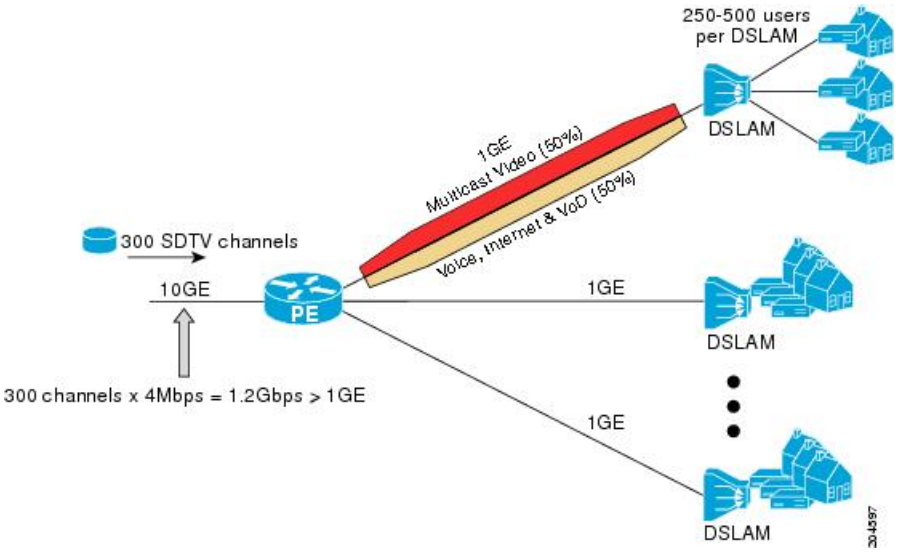
```
%MROUTE-4-ROUTELIMIT : 1501 routes exceeded multicast route-limit of 1500
```

Example: Configure IGMP state limiters

This example shows how to configure IGMP state limiters to provide multicast CAC in a network environment where all the multicast flows roughly utilize the same amount of bandwidth.

This example uses the topology illustrated in the figure. Although this illustration and example uses devices in the configuration, any device can be used.

Figure 1: IGMP state limit example topology



In this example, a service provider is offering 300 Standard Definition (SD) TV channels. Each SD channel utilizes approximately 4 Mbps.

The service provider must provision the Gigabit Ethernet interfaces on the PE device connected to the Digital Subscriber Line Access Multiplexers (DSLAMs) as follows: 50% of the link's bandwidth (500 Mbps) must be available to subscribers of the Internet, voice, and video on demand (VoD) service offerings while the remaining 50% (500 Mbps) of the link's bandwidth must be available to subscribers of the SD channel offerings.

Because each SD channel utilizes the same amount of bandwidth (4 Mbps), per interface IGMP state limiters can be used to provide the necessary CAC to provision the services being offered by the service provider. To determine the required CAC needed per interface, the total number of channels is divided by 4 (because each channel utilizes 4 Mbps of bandwidth). The required CAC needed per interface, therefore, is as follows:

500Mbps / 4Mbps = 125 mroutes

Once the required CAC is determined, the service provider uses the results to configure the per IGMP state limiters required to provision the Gigabit Ethernet interfaces on the PE device. Based on the network's CAC requirements, the service provider must limit the SD channels that can be transmitted out a Gigabit Ethernet interface (at any given time) to 125. Configuring a per interface IGMP state limit of 125 for the SD channels provisions the interface for 500 Mbps of bandwidth, the 50% of the link's bandwidth that must always be available (but never exceeded) for the SD channel offerings.

This configuration shows how the service provider uses a per interface mroute state limiter to provision interface Gigabit Ethernet 0/0/0 for the SD channels and Internet, Voice, and VoD services being offered to subscribers:

```
interface GigabitEthernet0/0/0
description --- Interface towards the DSLAM ---
.
.
.
ip igmp limit 125
```