Configuring MLD snooping

This chapter describes how to configure Multicast Listener Discovery (MLD) snooping on a Cisco NX-OS switch.

This chapter includes the following sections:

About MLD Snooping

Multicast Listener Discovery (MLD) snooping enables the efficient distribution of IPv6 multicast traffic between hosts and routers. It is a Layer 2 feature that restricts IPv6 multicast traffic within a bridge-domain to a subset of ports that have transmitted or received MLD queries or reports. In this way, MLD snooping provides the benefit of conserving the bandwidth on those segments of the network where no node has expressed interest in receiving the multicast traffic. This reduces the bandwidth usage instead of flooding the bridge-domain, and also helps hosts and routers save unwanted packet processing.

The MLD snooping functionality is similar to Internet Group Management Protocol (IGMP) snooping, except that the MLD snooping feature snoops for IPv6 multicast traffic and operates on MLDv1 (RFC 2710) and MLDv2 (RFC 3810) control plane packets. MLD is a sub-protocol of Internet Control Message Protocol version 6 (ICMPv6), so MLD message types are a subset of ICMPv6 messages and MLD messages are identified in IPv6 packets by a preceding next header value of 58. Message types in MLDv1 include listener queries, multicast address-specific (MAS) queries, listener reports, and done messages. MLDv2 is designed to be interoperable with MLDv1 except that it has an extra query type, the multicast address and source-specific (MASS) query. The protocol level timers available in MLD are similar to those available in IGMP.

When MLD snooping is disabled, then all the multicast traffic is flooded to all the ports, whether they have an interest or not. When MLD snooping is enabled, the fabric will forward IPv6 multicast traffic based on MLD interest. Unknown IPv6 multicast traffic will be flooded based on the bridge-domain's IPv6 L3 unknown multicast flood setting.

Flooding mode is used for forwarding unknown IPv6 multicast packets. In the flooding mode all endpoint groups (EPGs) and all ports under the bridge-domain will get the flooded packets.

Guidelines and Limitations for MLD Snooping

MLD snooping has the following guidelines and limitations:

- MLD snooping is supported on the following Cisco Nexus 3000 Series switches — N3K-C3132Q-V, N3K-C31108PC-V, N3K-C31108TC-V, N3K-C3132C-Z, N3K-C3264Q-S, N3K-C3232C, N3K-C3264C-E.
- For Cisco Nexus 3000 Series switches such as N3K-C3132Q-40GE, N3K-C3172PQ-10GE, N3K-C3172TQ-10GT along with their XL variants, an additional configuration of **system switch-mode n9k** command is required to support MLD snooping.
- If the below commands are configured, the MLD snooping configuration will be denied at the global level:
    - ip pim cpu-punt dr-only
    - ipv6 pim cpu-punt dr-only
    - ip pim non-dr flood
    - ipv6 pim non-dr flood

Configuring MLD Snooping

MLD snooping can be enabled and disabled in the global configuration mode as well as in the VLAN configuration mode. Snooping is disabled by default in the global configuration mode and enabled per VLAN. Snooping is operational on a VLAN only if it is enabled both on the VLAN as well is in the global configuration mode.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ipv6 mld snooping** **Example:** `switch(config)# ipv6 mld snooping`	Enables the admin state of the MLD snooping.
Step 3	**hardware access-list tcam region** *ing-sup tcam-size* **Example:**	Configures the TCAM region ing-sup to be 768 or more.

	Command or Action	Purpose
	`switch(config)# hardware access-list tcam region ing-sup 768`	**Note** After performing this step, you will be prompted to save the configuration and reboot the system for carving out the ACL and enable different hardware programming for v6 and v4 routerg.
Step 4	**ipv6 mld snooping explicit-tracking** **Example:** `switch(config)# ipv6 mld snooping explicit-tracking`	Enables or disables Explicit Host Tracking on a per VLAN basis. This command is enabled by default for both the MLD versions (v1 and v2).
Step 5	**ipv6 mld snooping report-suppression** **Example:** `switch(config)# ipv6 mld snooping report-suppression`	Enables or disables the report suppression. Every MLDv1 membership report received from the host is forwarded to all multicast router ports. When the report suppression is disabled, proxy reporting does not happen as all the MLD membership reports are forwarded to the router as is. This command is enabled by default.
Step 6	**ipv6 mld snooping v2-report-suppression** **Example:** `switch(config)# ipv6 mld snooping v2-report-suppression`	Enables MLDv2 report suppression. MLDv2 report suppression is disabled by default.
Step 7	**ipv6 mld snooping link-local-groups-suppression** **Example:** `switch(config)# ipv6 mld snooping link-local-groups-suppression`	Configures link-local-groups-suppression.

Step 8	**ipv6 mld snooping event-history vlan size** {**disabled** |**large** |**medium** |**small**}
	Example:
	`switch(config)# ipv6 mld snooping event-history vlan size medium`
		Configures event history buffers for VLANs. Default value is medium.

Step 9	**ipv6 mld snooping event-history vlan-events** {**disabled** |**large** |**medium** |**small**}
	Example:
	`switch(config)# ipv6 mld snooping event-history vlan-events medium`
		Configures event history buffers for VLAN events. Default value is medium.

Step 10	**ipv6 mld snooping event-history MLD-snoop-internal size** {**disabled** |**large** |**medium** |**small**} **Example:**	Configures event history buffers for MLD-snoop internal events. Default value is small.

	Command or Action	Purpose
	`switch(config)# ipv6 mld snooping event-history MLD-snoop-internal size small`	

Step 11	**ipv6 mld snooping event-history mfdm size** {**disabled** |**large** |**medium** |**small**}
	Example:
	`switch(config)# ipv6 mld snooping event-history mfdm size small`
		Configures event history buffers for MLD-snoop MFDM events. Default value is small.

Step 12	**ipv6 mld snooping event-history mfdm-sum** {**disabled** |**large** |**medium** |**small**}
	Example:
	`switch(config)# ipv6 mld snooping event-history mfdm-sum size small`
		Configures event history buffers for MLD-snoop MFDM event summary. Default value is small.

Step 13	**ipv6 mld snooping event-history vpc size** {**disabled** |**large** |**medium** |**small**}
	Example:
	`switch(config)# ipv6 mld snooping event-history vpc size small`
		Configures event history buffers for MLD-snoop vPC events. Default value is small.

Step 14	**vlan configuration** *vlan-id* **Example:** `switch(config)# vlan configuration 6`	Enters VLAN configuration mode.
Step 15	**[no] ipv6 mld snooping** **Example:** `switch(config-vlan)# no ipv6 mld snooping`	Disables or enables MLD snooping per VLAN. Once disabled, PIM6 will not work on the corresponding “interface vlan”.
Step 16	**ipv6 mld snooping fast-leave** **Example:** `switch(config-vlan)# ipv6 mld snooping fast-leave`	Allows you to turn on or off the fast-leave feature on a per-VLAN basis. This applies to MLDv2 hosts and is used on ports that are known to have only one host doing MLD behind that port. This command is disabled by default. This is a VLAN mode command.
Step 17	**ipv6 mld snooping mrouter interface** *interface-identifier* **Example:** `switch(config-vlan)# ipv6 mld snooping mrouter interface port-channel 1`	Specifies a static connection to a multicast router. The interface to the router must be in the VLAN where the command is entered and must be administratively up along with the line protocol. This is a VLAN mode command.
Step 18	**ipv6 mld snooping static-group** *group* [**source** *source*] **interface** *interface-identifier* **Example:**	Configures a Layer2 port on a specific VLAN as a member of a multicast group statically. This is a VLAN mode command.

	Command or Action	Purpose
	`switch(config-vlan)# ipv6 mld snooping static-group ff1e::abcd interface port-channel 2`	
Step 19	**ipv6 mld snooping last-member-query-interval** [*interval*] **Example:** `switch(config-vlan)# ipv6 mld snooping last-member-query-interval 9`	Configures the interval for which the switch waits after sending a group-specific query to determine if hosts are still interested in a specific multicast group. It configures the interval for the MLD queries sent by the switch. Default is 1 second. Valid range is 1 to 25 seconds. This is a VLAN mode command. When both MLD fast-leave processing and the MLD query interval are configured, fast-leave processing is considered as the priority.
Step 20	**ipv6 mld snooping querier** *link-local address* **Example:** `switch(config-vlan)# ipv6 mld snooping querier aaaa::abcd`	Enables or disables IPv6 MLD snooping querier processing. MLD snooping querier supports the MLD snooping in a VLAN where PIM and MLD are not configured because the multicast traffic does not need to be routed.

Verifying the MLD Snooping Configuration

To display the MLD snooping configuration information, perform one of the following tasks:

show ipv6 mld snooping [**vlan** *vlan-id*]	Displays the MLD snooping status and details for a given VLAN or all VLANs.
show ipv6 mld snooping mrouter [**vlan** *vlan-id*]	Displays the multicast router ports in each VLAN.
show ipv6 mld snooping querier [**vlan** *vlan-id*]	Displays details on the MLD Querier for the VLAN in which MLD Snooping is enabled.
show ipv6 mld snooping explicit-tracking vlan *vlan-id*	Displays the MLD snooping explicit tracking information.
show ipv6 mld snooping statistics global	Displays the global MLD snooping statistics.

show ipv6 mld snooping groups [**vlan** *vlan-id*] [**detail**]	Displays groups, the type of reports that are received for the group (host type) and the list of ports on which reports are received. The list of ports does not include the multicast router ports. This represents the list of ports on which the reports have been received and not the complete forwarding port set for the group. Displays the router ports by the */* entry in the non-detailed output.