Implementing MLD Snooping

This module describes how to implement MLD snooping on the Cisco ASR 9000 Series Router.

Feature History for MLD Snooping

Release	Modification
Release 4.3.0	This feature was introduced.

MLD Snooping

Multicast Listener Discovery (MLD) snooping provides a way to constrain multicast traffic at Layer 2. By snooping the MLD membership reports sent by hosts in the bridge domain, the MLD snooping application can set up Layer 2 multicast forwarding tables to deliver traffic only to ports with at least one interested member, significantly reducing the volume of multicast traffic.

MLD snooping uses the information in MLD membership report messages to build corresponding information in the forwarding tables to restrict IPv6 multicast traffic at Layer 2. The forwarding table entries are in the form <Route, OIF List>, where:

- Route is a <*, G> route or <S, G> route.
- OIF List comprises all bridge ports that have sent MLD membership reports for the specified route plus all multicast router (mrouter) ports in the bridge domain.

For more information regarding MLD snooping, refer the *Multicast Configuration Guide for Cisco ASR 9000 Series Routers*.

Prerequisites for MLD Snooping

- The network must be configured with a layer2 VPN.
- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Restrictions for MLD Snooping

Following are the restrictions (features that are not supported):

- MLD Snooping is supported only on L2VPN bridge domains.
- Explicit host tracking.
- Multicast Admission Control.
- Security filtering.
- Report rate limiting.
- Multicast router discovery.

Advantages of MLD Snooping

Advantages of MLD Snooping

- In its basic form, it reduces bandwidth consumption by reducing multicast traffic that would otherwise flood an entire VPLS bridge domain.
- With the use of some optional configurations, it provides security between bridge domains by filtering the MLD reports received from hosts on one bridge port and preventing leakage towards the hosts on other bridge ports.

High Availability (HA) features for MLD

MLD supports the following HA features:

- Process restarts
- RP Failover
- Stateful Switch-Over (SSO)
- Non-Stop Forwarding (NSF)—Forwarding continues unaffected while the control plane is restored following a process restart or route processor (RP) failover.
- Line card online insertion and removal (OIR)

Bridge Domain Support for MLD

MLD snooping operates at the bridge domain level. When MLD snooping is enabled on a bridge domain, the snooping functionality applies to all ports under the bridge domain, including:

- Physical ports under the bridge domain.
- Ethernet flow points (EFPs)—An EFP can be a VLAN, VLAN range, list of VLANs, or an entire interface port.
- Pseudowires (PWs) in VPLS bridge domains.
- Ethernet bundles—Ethernet bundles include IEEE 802.3ad link bundles and Cisco EtherChannel bundles. From the perspective of the MLD snooping application, an Ethernet bundle is just another EFP. The forwarding application in the Cisco ASR 9000 Series Routers randomly nominates a single port from the bundle to carry the multicast traffic.

Multicast Router and Host Ports

MLD snooping classifies each port as one of the following:

- Multicast router ports (mrouter ports)—These are ports to which a multicast-enabled router is connected. Mrouter ports are usually dynamically discovered, but may also be statically configured. Multicast traffic is always forwarded to all mrouter ports, except when an mrouter port is the ingress port.
- Host ports—Any port that is not an mrouter port is a host port.

Multicast Router Discovery for MLD

MLD snooping discovers mrouter ports dynamically. You can also explicitly configure a port as an emrouter port.

- Discovery- MLD snooping identifies upstream mrouter ports in the bridge domain by snooping mld query messages and Protocol Independent Multicast Version 2 (PIMv2) hello messages. Snooping PIMv2 hello messages identifies mld nonqueriers in the bridge domain.
- Static configuration—You can statically configure a port as an mrouter port with the **mrouter** command in a profile attached to the port. Static configuration can help in situations when incompatibilities with non-Cisco equipment prevent dynamic discovery.

Multicast Traffic Handling for MLD

The following tables describe the traffic handling behavior by MLD mrouters and host ports.

Table 1: Multicast Traffic Handling for a MLDv1 Querier

Traffic Type	Received on MRouter Ports	Received on Host Ports
IP multicast source traffic	Forwards to all mrouter ports and to host ports that indicate interest.	Forwards to all mrouter ports and to host ports that indicate interest.
MLD general queries	Forwards to all ports.	—
MLD group-specific queries	Forwards to all other mrouter ports.	Dropped
MLDv1 joins	Examines (snoops) the reports. • If report suppression is enabled, forwards first join for a new group or first join following a general query for an existing group. • If report suppression is disabled, forwards on all mrouter ports.	Examines (snoops) the reports. • If report suppression is enabled, forwards first join for a new group or first join following a general query for an existing group. • If report suppression is disabled, forwards on all mrouter ports.
MLDv2 reports	Ignores	Ignores
MLDv1 leaves	Invokes last member query processing.	Invokes last member query processing.

Table 2: Multicast Traffic Handling for a MLDv2 Querier

Traffic Type	Received on MRouter Ports	Received on Host Ports
IP multicast source traffic	Forwards to all mrouter ports and to host ports that indicate interest.	Forwards to all mrouter ports and to host ports that indicate interest.
MLD general queries	Forwards to all ports.	—
MLD group-specific queries	If received on the querier port floods on all ports.	—
MLDv1 joins	Handles as MLDv2 IS_EX{} reports.	Handles as MLDv2 IS_EX{} reports.

Traffic Type	Received on MRouter Ports	Received on Host Ports
MLDv2 reports	• If proxy reporting is enabled—For state changes or source-list changes, generates a state change report on all mrouter ports. • If proxy reporting is disabled—Forwards on all mrouter ports.	• If proxy reporting is enabled—For state changes or source-list changes, generates a state change report on all mrouter ports. • If proxy reporting is disabled—Forwards on all mrouter ports.
MLDv1 leaves	Handles as MLDv2 IS_IN{} reports.	Handles as MLDv2 IS_IN{} reports.

Creating a MLD Snooping Profile

SUMMARY STEPS

1. **configure**
2. **mld snooping profile** *profile-name*
3. Optionally, add commands to override default configuration values.
4. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mld snooping profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config)# mld snooping profile default-bd-profile`	Enters MLD snooping profile configuration mode and creates a named profile. The default profile enables MLD snooping. You can commit the new profile without any additional configurations, or you can include additional configuration options to the profile. You can also return to the profile later to add configurations, as described in other tasks in this module.
Step 3	Optionally, add commands to override default configuration values.	If you are creating a bridge domain profile, consider the following: • An empty profile is appropriate for attaching to a bridge domain. An empty profile enables MLD snooping with default configuration values. • You can optionally add more commands to the profile to override default configuration values. • If you include port-specific configurations in a bridge domain profile, the configurations apply to all ports under the bridge, unless another profile is attached to a port.

	Command or Action	Purpose
		If you are creating a port-specific profile, consider the following: • While an empty profile could be attached to a port, it would have no effect on the port configuration. • When you attach a profile to a port, MLD snooping reconfigures that port, overriding any inheritance of configuration values from the bridge-domain profile. You must repeat the commands in the port profile if you want to retain those configurations. You can detach a profile, change it, and reattach it to add commands to a profile at a later time.
Step 4	**commit**	

Activating MLD Snooping on a Bridge Domain

To activate MLD snooping on a bridge domain, attach a MLD snooping profile to the desired bridge domain as explained here.

SUMMARY STEPS

1. **configure**
2. **l2vpn**
3. **bridge group** *bridge-group-name*
4. **bridge-domain** *bridge-domain-name*
5. **mld snooping profile** *profile-name*
6. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**l2vpn** **Example:** `RP/0/RSP0/CPU0:router(config)# l2vpn`	Enters Layer 2 VPN configuration mode.
Step 3	**bridge group** *bridge-group-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group GRP1`	Enters Layer 2 VPN VPLS bridge group configuration mode for the named bridge group.

	Command or Action	Purpose
Step 4	**bridge-domain** *bridge-domain-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain ISP1`	Enters Layer 2 VPN VPLS bridge group bridge domain configuration mode for the named bridge domain.
Step 5	**mld snooping profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# mld snooping profile default-bd-profile`	Attaches the named MLD snooping profile to the bridge domain, enabling MLD snooping on the bridge domain.
Step 6	**commit**	

Deactivating MLD Snooping on a Bridge Domain

To deactivate MLD snooping from a bridge domain, remove the profile from the bridge domain using the following steps:

Note A bridge domain can have only one profile attached to it at a time.

SUMMARY STEPS

1. **configure**
2. **l2vpn**
3. **bridge group** *bridge-group-name*
4. **bridge-domain** *bridge-domain-name*
5. **no mld snooping**
6. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**l2vpn** **Example:** `RP/0/RSP0/CPU0:router(config)# l2vpn`	Enters Layer 2 VPN configuration mode.
Step 3	**bridge group** *bridge-group-name* **Example:**	Enters Layer 2 VPN VPLS bridge group configuration mode for the named bridge group.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group GRP1`	
Step 4	**bridge-domain** *bridge-domain-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain ISP1`	Enters Layer 2 VPN VPLS bridge group bridge domain configuration mode for the named bridge domain.
Step 5	**no mld snooping** **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# no mld snooping`	Detaches the MLD snooping profile from the bridge domain, disabling MLD snooping on that bridge domain. **Note** Only one profile can be attached to a bridge domain at a time. If a profile is attached, MLD snooping is enabled. If a profile is not attached, MLD snooping is disabled.
Step 6	**commit**	

Configuring Static Mrouter Ports (MLD)

Before you begin

MLD snooping must be enabled on the bridge domain for port-specific profiles to affect MLD snooping behavior.

Note Static mrouter port configuration is a port-level option and should be added to profiles intended for ports. It is not recommended to add mrouter port configuration to a profile intended for bridge domains.

SUMMARY STEPS

1. **configure**
2. **mld snooping profile** *profile-name*
3. **mrouter**
4. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mld snooping profile** *profile-name* **Example:**	Enters MLD snooping profile configuration mode and creates a new profile or accesses an existing profile.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config)# mld snooping profile mrouter-port-profile`	
Step 3	**mrouter** **Example:** `RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# mrouter`	Configures a port as a static mrouter port.
Step 4	**commit**	

Configuring Router Guard (MLD)

To prevent multicast routing protocol messages from being received on a port and, therefore, prevent a port from being a dynamic mrouter port, follow these steps. Note that both router guard and static mrouter commands may be configured on the same port.

Before you begin

MLD snooping must be enabled on the bridge domain for port-specific profiles to affect MLD snooping behavior.

Note Router guard configuration is a port-level option and should be added to profiles intended for ports. It is not recommended to add router guard configuration to a profile intended for bridge domains. To do so would prevent all mrouters, including MLD queriers, from being discovered in the bridge domain.

SUMMARY STEPS

1. **configure**
2. **mld snooping profile** *profile-name*
3. **router-guard**
4. **commit**
5. **show mld snooping profile** *profile-name* **detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mld snooping profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config)# mld snooping profile`	Enters MLD snooping profile configuration mode and creates a new profile or accesses an existing profile.

	Command or Action	Purpose
	`host-port-profile`	
Step 3	**router-guard** **Example:** `RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# router-guard`	Protects the port from dynamic discovery.
Step 4	**commit**	
Step 5	**show mld snooping profile** *profile-name* **detail** **Example:** `RP/0/RSP0/CPU0:router# show mld snooping profile host-port-profile detail`	(Optional) Displays the configuration settings in the named profile.

Configuring Immediate-leave for MLD

To add the MLD snooping immediate-leave option to an MLD snooping profile, follow these steps.

SUMMARY STEPS

1. **configure**
2. **mld snooping profile** *profile-name*
3. **immediate-leave**
4. **commit**
5. **show mld snooping profile** *profile-name* **detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mld snooping profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config)# mld snooping profile host-port-profile`	Enters MLD snooping profile configuration mode and creates a new profile or accesses an existing profile.
Step 3	**immediate-leave** **Example:** `RP/0/RSP0/CPU0:router(config-mld-snooping-profile)#`	Enables the immediate-leave option. • If you add this option to a profile attached to a bridge domain, it applies to all ports under the bridge.

	Command or Action	Purpose
	`immediate-leave`	• If you add this option to a profile attached to a port, it applies to the port.
Step 4	**commit**	
Step 5	**show mld snooping profile** *profile-name* **detail** **Example:** `RP/0/RSP0/CPU0:router# show mld snooping profile host-port-profile detail`	(Optional) Displays the configuration settings in the named profile.

Configuring Internal Querier for MLD

Before you begin

MLD snooping must be enabled on the bridge domain for this procedure to take effect.

SUMMARY STEPS

1. **configure**
2. **mld snooping profile** *profile-name*
3. **system-ip-address** *ip-addr*
4. **internal-querier**
5. **commit**
6. **show mld snooping profile** *profile-name* **detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mld snooping profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config)# mld snooping profile internal-querier-profile`	Enters MLD snooping profile configuration mode and creates a new profile or accesses an existing profile.
Step 3	**system-ip-address** *ip-addr* **Example:** `RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# system-ip-address 10.1.1.1`	Configures an IP address for internal querier use. The default system-ip-address value (0.0.0.0) is not valid for the internal querier. You must explicitly configure an IP address.

	Command or Action	Purpose
Step 4	**internal-querier** **Example:** `RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# internal-querier`	Enables an internal querier with default values for all options.
Step 5	**commit**	
Step 6	**show mld snooping profile** *profile-name* **detail** **Example:** `RP/0/RSP0/CPU0:router# show mld snooping profile internal-querier-profile detail`	(Optional) Displays the configuration settings in the named profile.

Configuring Static Groups for MLD

To add one or more static groups or MLDv2 source groups to an MLD snooping profile, follow these steps.

Before you begin

MLD snooping must be enabled on the bridge domain for port-specific profiles to affect MLD snooping behavior.

SUMMARY STEPS

1. **configure**
2. **mld snooping profile** *profile-name*
3. **static-group** *group-addr* [**source** *source-addr*]
4. Repeat the previous step, as needed, to add more static groups.
5. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mld snooping profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config)# mld snooping profile host-port-profile`	Enters MLD snooping profile configuration mode and creates a new profile or accesses an existing profile.
Step 3	**static-group** *group-addr* [**source** *source-addr*] **Example:**	Configures a static group.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# static-group 239.1.1.1 source 10.0.1.1`	• If you add this option to a profile attached to a bridge domain, it applies to all ports under the bridge. • If you add this option to a profile attached to a port, it applies to the port.
Step 4	Repeat the previous step, as needed, to add more static groups.	(Optional) Adds additional static groups.
Step 5	**commit**	

Configuring MLD Snooping

1. Create two profiles:

```
mld snooping profile bridge_profile
!
mld snooping profile port_profile
   mrouter
!
```

2. Configure two physical interfaces for L2 support.

```
interface GigabitEthernet0/8/0/38
   negotiation auto
   l2transport
   no shut
   !
!
interface GigabitEthernet0/8/0/39
   negotiation auto
   l2transport
   no shut
   !
!
```

3. Add interfaces to the bridge domain. Attach bridge_profile to the bridge domain and port_profile to one of the Ethernet interfaces. The second Ethernet interface inherits MLD snooping configuration attributes from the bridge domain profile.

```
l2vpn
  bridge group bg1
     bridge-domain bd1
     mld snooping profile bridge_profile
     interface GigabitEthernet0/8/0/38
       mld snooping profile port_profile
     interface GigabitEthernet0/8/0/39
     !
  !
!
```

4. Verify the configured bridge ports.

```
show mld snooping port
```

Configuring MLD Snooping on Ethernet Bundles

1. This example assumes that the front-ends of the bundles are preconfigured. For example, a bundle configuration might consist of three switch interfaces, as follows:

```
    interface Port-channel1
    !
interface GigabitEthernet0/0/0/0
    !
interface GigabitEthernet0/0/0/1
!
    interface GigabitEthernet0/0/0/2
       channel-group 1 mode on
    !
    interface GigabitEthernet0/0/0/3
       channel-group 1 mode on
    !
```

2. Configure two MLD snooping profiles.

```
       mld snooping profile bridge_profile
       !
       mld snooping profile port_profile
          mrouter
       !
```

3. Configure interfaces as bundle member links.

```
       interface GigabitEthernet0/0/0/0
         bundle id 1 mode on
         negotiation auto
       !
       interface GigabitEthernet0/0/0/1
         bundle id 1 mode on
         negotiation auto
       !
       interface GigabitEthernet0/0/0/2
         bundle id 2 mode on
         negotiation auto
       !
       interface GigabitEthernet0/0/0/3
         bundle id 2 mode on
         negotiation auto
       !
```

4. Configure the bundle interfaces for L2 transport.

```
interface Bundle-Ether 1
          l2transport
          !
       !
```

```
interface Bundle-Ether 2
   l2transport
   !
!
```

5. Add the interfaces to the bridge domain and attach MLD snooping profiles.

```
l2vpn
  bridge group bg1
     bridge-domain bd1
     mld snooping profile bridge_profile
     interface bundle-Ether 1
       mld snooping profile port_profile
     interface bundle-Ether 2
     !
   !
!
```

6. Verify the configured bridge ports.

```
show mld snooping port
```