

# 目 录

1 MLD Snooping.....	1-1
1.1 MLD Snooping简介 .....	1-1
1.1.1 MLD Snooping原理 .....	1-1
1.1.2 MLD Snooping基本概念 .....	1-2
1.1.3 MLD Snooping工作机制 .....	1-3
1.1.4 协议规范 .....	1-4
1.2 MLD Snooping配置任务简介.....	1-5
1.3 配置MLD Snooping基本功能.....	1-5
1.3.1 配置准备 .....	1-5
1.3.2 使能MLD Snooping .....	1-6
1.3.3 配置MLD Snooping版本 .....	1-6
1.3.4 配置MLD Snooping转发表项的全局最大数量.....	1-7
1.4 配置MLD Snooping端口功能.....	1-8
1.4.1 配置准备 .....	1-8
1.4.2 配置动态端口老化定时器 .....	1-8
1.4.3 配置静态端口 .....	1-9
1.4.4 配置模拟主机加入 .....	1-10
1.4.5 配置端口快速离开 .....	1-10
1.5 配置MLD Snooping查询器 .....	1-11
1.5.1 配置准备 .....	1-11
1.5.2 使能MLD Snooping查询器.....	1-11
1.5.3 配置MLD查询和响应.....	1-12
1.6 调整MLD报文 .....	1-13
1.6.1 配置准备 .....	1-13
1.6.2 配置MLD报文的源IPv6 地址 .....	1-13
1.7 配置MLD Snooping策略.....	1-14
1.7.1 配置准备 .....	1-14
1.7.2 配置IPv6 组播组过滤器.....	1-14
1.7.3 配置丢弃未知IPv6 组播数据报文 .....	1-15
1.7.4 配置MLD成员关系报告报文抑制.....	1-16
1.7.5 配置端口加入的IPv6 组播组最大数量.....	1-16
1.7.6 配置IPv6 组播组替换功能 .....	1-17
1.8 MLD Snooping显示和维护 .....	1-18

1.9 MLD Snooping典型配置举例.....	1-19
1.9.1 IPv6 组策略及模拟主机加入配置举例.....	1-19
1.9.2 静态端口配置举例.....	1-21
1.9.3 MLD Snooping查询器配置举例.....	1-24
1.10 常见配置错误举例.....	1-27
1.10.1 二层设备不能实现二层组播.....	1-27
1.10.2 配置的IPv6 组播组策略不生效.....	1-27

# 1 MLD Snooping



说明

设备支持两种运行模式：独立运行模式和 IRF 模式，缺省情况下为独立运行模式。有关 IRF 模式的介绍，请参见“虚拟化技术配置指导”中的“IRF”。

## 1.1 MLD Snooping简介

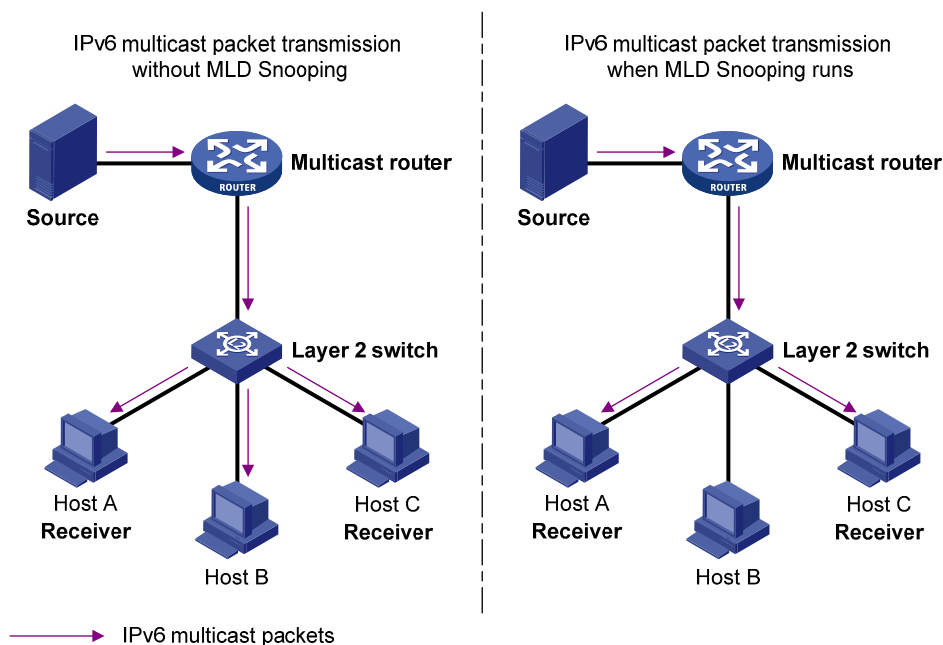
MLD Snooping（Multicast Listener Discovery Snooping，组播侦听者发现协议窥探）运行在二层设备上，通过侦听三层设备与主机之间的 MLD 报文来生成二层组播转发表，从而管理和控制 IPv6 组播数据报文的转发，实现 IPv6 组播数据报文在二层的按需分发。

### 1.1.1 MLD Snooping原理

运行 MLD Snooping 的二层设备通过对收到的 MLD 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发 IPv6 组播数据。

如 [图 1-1](#) 所示，当二层设备没有运行 MLD Snooping 时，IPv6 组播数据报文在二层网络中被广播；当二层设备运行了 MLD Snooping 后，已知 IPv6 组播组的组播数据报文不会在二层网络中被广播，而被组播给指定的接收者。

图1-1 二层设备运行 MLD Snooping 前后的对比



MLD Snooping 通过二层组播将信息只转发给有需要的接收者，可以带来以下好处：

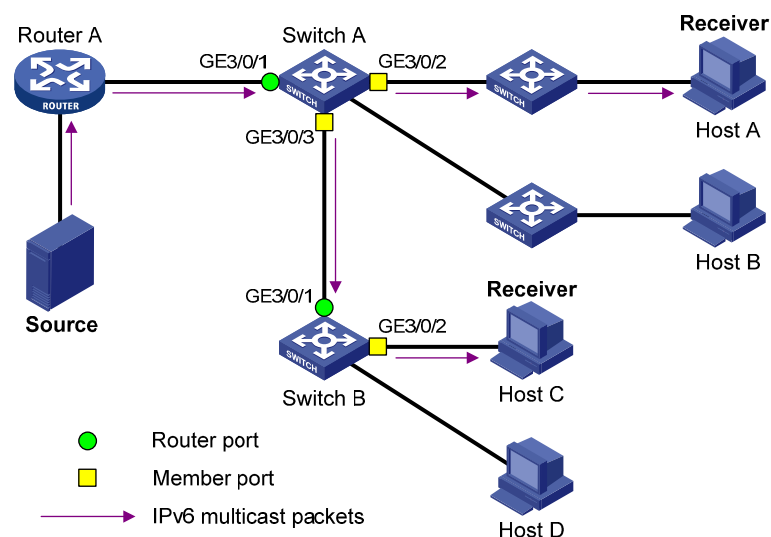
- 减少了二层网络中的广播报文，节约了网络带宽；
- 增强了 IPv6 组播信息的安全性；
- 为实现对每台主机的单独计费带来了方便。

## 1.1.2 MLD Snooping基本概念

### 1. MLD Snooping相关端口

如 [图 1-2](#) 所示，Router A 连接 IPv6 组播源，在 Switch A 和 Switch B 上分别运行 MLD Snooping，Host A 和 Host C 为接收者主机（即 IPv6 组播组成员）。

图1-2 MLD Snooping 相关端口



结合 [图 1-2](#)，介绍一下 MLD Snooping 相关的端口概念：

- 路由器端口（Router Port）：二层设备上朝向三层组播设备（DR 或 MLD 查询器）一侧的端口，如 Switch A 和 Switch B 各自的 GigabitEthernet 3/0/1 端口。二层设备将本设备上的所有路由器端口都记录在路由器端口列表中。
- 成员端口（Member Port）：又称 IPv6 组播组成员端口，表示二层设备上朝向 IPv6 组播组成员一侧的端口，如 Switch A 的 GigabitEthernet3/0/2 和 GigabitEthernet3/0/3 端口，以及 Switch B 的 GigabitEthernet3/0/2 端口。二层设备将本设备上的所有成员端口都记录在 MLD Snooping 转发表中。



#### 说明

- 本文中提到的路由器端口都是指二层设备上朝向三层组播设备的端口，而不是指路由器上的端口。
- 如不特别说明，本文中提到的路由器/成员端口均包括动态和静态端口。
- 在运行了 MLD Snooping 的二层设备上，所有收到源地址不为 0::0 的 MLD 普遍组查询报文或 IPv6 PIM Hello 报文的端口都将被视为动态路由器端口。有关 IPv6 PIM Hello 报文的详细介绍，请参见“IP 组播配置指导”中的“IPv6 PIM”。

## 2. MLD Snooping动态端口老化定时器

表1-1 MLD Snooping 动态端口老化定时器

定时器	说明	超时前应收到的报文	超时后二层设备的动作
动态路由器端口老化定时器	二层设备为其每个动态路由器端口都启动一个定时器，其超时时间就是动态路由器端口老化时间	源地址不为0::0的MLD普遍组查询报文或IPv6 PIM Hello报文	将该端口从路由器端口列表中删除
动态成员端口老化定时器	当一个端口动态加入某IPv6组播组时，二层设备为该端口启动一个定时器，其超时时间就是动态成员端口老化时间	MLD成员关系报告报文	将该端口从MLD Snooping转发表中删除



说明

MLD Snooping 端口老化机制只针对动态端口，静态端口永不老化。

### 1.1.3 MLD Snooping工作机制

运行了 MLD Snooping 的二层设备对不同 MLD 动作的具体处理方式如下：



说明

本节中所描述的增删端口动作均只针对动态端口，静态端口只能通过相应的配置进行增删，具体步骤请参见“[1.4.3 配置静态端口](#)”。

#### 1. 普遍组查询

MLD 查询器定期向本地网段内的所有主机与路由器（FF02::1）发送 MLD 普遍组查询报文，以查询该网段有哪些 IPv6 组播组的成员。

在收到 MLD 普遍组查询报文时，二层设备将其通过 VLAN 内除接收端口以外的其它所有端口转发出去，并对该报文的接收端口做如下处理：

- 如果在路由器端口列表中已包含该动态路由器端口，则重置其老化定时器。
- 如果在路由器端口列表中尚未包含该动态路由器端口，则将其添加到路由器端口列表中，并启动其老化定时器。

#### 2. 报告成员关系

以下情况，主机会向 MLD 查询器发送 MLD 成员关系报告报文：

- 当 IPv6 组播组的成员主机收到 MLD 查询报文后，会回复 MLD 成员关系报告报文。
- 如果主机要加入某个 IPv6 组播组，它会主动向 MLD 查询器发送 MLD 成员关系报告报文以声明加入该 IPv6 组播组。

在收到 MLD 成员关系报告报文时，二层设备将其通过 VLAN 内的所有路由器端口转发出去，从该报文中解析出主机要加入的 IPv6 组播组地址，并对该报文的接收端口做如下处理：

- 如果不存在该 IPv6 组播组所对应的转发表项，则创建转发表项，将该端口作为动态成员端口添加到出端口列表中，并启动其老化定时器；

- 如果已存在该 IPv6 组播组所对应的转发表项，但其出端口列表中不包含该端口，则将该端口作为动态成员端口添加到出端口列表中，并启动其老化定时器；
- 如果已存在该 IPv6 组播组所对应的转发表项，且其出端口列表中已包含该动态成员端口，则重置其老化定时器。



二层设备不会将 MLD 成员关系报告报文通过非路由器端口转发出去，因为根据主机上的 MLD 成员关系报告抑制机制，如果非路由器端口下还有该 IPv6 组播组的成员主机，则这些主机在收到该报告报文后便抑制了自身的报告，从而使二层设备无法获知这些端口下还有该 IPv6 组播组的成员主机。有关主机上的 MLD 成员关系报告抑制机制的详细介绍，请参见“IP 组播配置指导”中的“MLD”。

### 3. 离开组播组

当主机离开 IPv6 组播组时，会通过发送 MLD 离开组报文，以通知三层组播设备自己离开了某个 IPv6 组播组。当二层设备从某动态成员端口上收到 MLD 离开组报文时，首先判断要离开的 IPv6 组播组所对应的转发表项是否存在，以及该 IPv6 组播组所对应转发表项的出端口列表中是否包含该接收端口：

- 如果不存在该 IPv6 组播组对应的转发表项，或者该 IPv6 组播组对应转发表项的出端口列表中不包含该端口，二层设备不会向任何端口转发该报文，而将其直接丢弃；
- 如果存在该 IPv6 组播组对应的转发表项，且该 IPv6 组播组对应转发表项的出端口列表中包含该端口，二层设备会将该报文通过 VLAN 内的所有路由器端口转发出去。同时，由于并不知道该接收端口下是否还有该 IPv6 组播组的其它成员，所以二层设备不会立刻把该端口从该 IPv6 组播组所对应转发表项的出端口列表中删除，而是调整该端口的老化定时器。

当 MLD 查询器收到 MLD 离开组报文后，从中解析出主机要离开的 IPv6 组播组的地址，并通过接收端口向该 IPv6 组播组发送 MLD 特定组查询报文。二层设备在收到 MLD 特定组查询报文后，将其通过 VLAN 内的所有路由器端口和该 IPv6 组播组的所有成员端口转发出去。对于 MLD 离开组报文的接收端口（假定为动态成员端口），二层设备在其老化时间内：

- 如果从该端口收到了主机响应该特定组查询的 MLD 成员关系报告报文，则表示该端口下还有该 IPv6 组播组的成员，于是重置其老化定时器；
- 如果没有从该端口收到主机响应该特定组查询的 MLD 成员关系报告报文，则表示该端口下已没有该 IPv6 组播组的成员。当该端口的老化定时器超时后，将其从该 IPv6 组播组所对应转发表项的出端口列表中删除。

#### 1.1.4 协议规范

与 MLD Snooping 相关的协议规范有：

- RFC 4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

## 1.2 MLD Snooping配置任务简介

表1-2 MLD Snooping 配置任务简介

	配置任务	说明	详细配置
配置MLD Snooping基本功能	使能MLD Snooping	必选	<a href="#">1.3.2</a>
	配置MLD Snooping版本	可选	<a href="#">1.3.3</a>
	配置MLD Snooping转发表项的全局最大数量	可选	<a href="#">1.3.4</a>
配置MLD Snooping端口功能	配置动态端口老化定时器	可选	<a href="#">1.4.2</a>
	配置静态端口	可选	<a href="#">1.4.3</a>
	配置模拟主机加入	可选	<a href="#">1.4.3</a>
	配置端口快速离开	可选	<a href="#">1.4.5</a>
配置MLD Snooping查询器	使能MLD Snooping查询器	可选	<a href="#">1.5.2</a>
	配置MLD查询和响应	可选	<a href="#">1.5.3</a>
调整MLD报文	配置MLD报文的源IPv6地址	可选	<a href="#">1.6.2</a>
配置MLD Snooping策略	配置IPv6组播组过滤器	可选	<a href="#">1.7.2</a>
	配置丢弃未知IPv6组播数据报文	可选	<a href="#">1.7.3</a>
	配置MLD成员关系报告报文抑制	可选	<a href="#">1.7.4</a>
	配置端口加入的 IPv6 组播组最大数量	可选	<a href="#">1.7.5</a>
	配置IPv6组播组替换功能	可选	<a href="#">1.7.6</a>

### 说明

- 对于从 Secondary VLAN 中收到的主机加入请求，相关的 MLD Snooping 转发表项都将维护在 Primary VLAN 中，因此 MLD Snooping 功能只需在 Primary VLAN 中配置即可，在 Secondary VLAN 中即使配置了也不会生效。有关 Primary VLAN 和 Secondary VLAN 的详细介绍，请参见“二层技术-以太网交换配置指导”中的“VLAN”。
- 二层聚合接口与其各成员端口上的配置互不影响，且成员端口上的配置只有当该端口退出聚合组后才会生效，二层聚合接口上的配置也不会参与聚合计算。

## 1.3 配置MLD Snooping基本功能

### 1.3.1 配置准备

在配置 MLD Snooping 基本功能之前，需完成以下任务：

- 配置相应 VLAN

在配置 MLD Snooping 基本功能之前，需准备以下数据：

- MLD Snooping 的版本
- MLD Snooping 转发表项的全局最大数量

### 1.3.2 使能MLD Snooping

在 VLAN 内使能 MLD Snooping 之前，必须先全局使能 MLD Snooping。在 VLAN 内使能了 MLD Snooping 之后，MLD Snooping 只在属于该 VLAN 的端口上生效。

用户既可在 MLD-Snooping 视图下对指定 VLAN 进行配置，也可在 VLAN 视图下只对当前 VLAN 进行配置，二者的配置优先级相同。

#### 1. 使能指定VLAN内的MLD Snooping

表1-3 在 VLAN 内使能 MLD Snooping

操作	命令	说明
进入系统视图	<b>system-view</b>	-
全局使能MLD Snooping，并进入 MLD-Snooping视图	<b>mld-snooping</b>	缺省情况下，MLD Snooping处于关闭状态
使能指定VLAN内的MLD Snooping	<b>enable vlan <i>vlan-list</i></b>	缺省情况下，VLAN内的MLD Snooping处于关闭状态

#### 2. 在VLAN内使能MLD Snooping

表1-4 在 VLAN 内使能 MLD Snooping

操作	命令	说明
进入系统视图	<b>system-view</b>	-
全局使能MLD Snooping，并进入 MLD-Snooping视图	<b>mld-snooping</b>	缺省情况下，MLD Snooping处于关闭状态
退回系统视图	<b>quit</b>	-
进入VLAN视图	<b>vlan <i>vlan-id</i></b>	-
在VLAN内使能MLD Snooping	<b>mld-snooping enable</b>	缺省情况下，VLAN内的MLD Snooping处于关闭状态

### 1.3.3 配置MLD Snooping版本

配置 MLD Snooping 的版本，实际上就是配置 MLD Snooping 可以处理的 MLD 报文的版本：

- 当 MLD Snooping 的版本为 1 时，MLD Snooping 能够对 MLDv1 的报文进行处理，对 MLDv2 的报文则不进行处理，而是在 VLAN 内将其广播；
- 当 MLD Snooping 的版本为 2 时，MLD Snooping 能够对 MLDv1 和 MLDv2 的报文进行处理。

用户既可在 MLD-Snooping 视图下对指定 VLAN 进行配置，也可在 VLAN 视图下只对当前 VLAN 进行配置，二者的配置优先级相同。



## 1. 配置指定VLAN内的MLD Snooping版本

表1-5 配置指定 VLAN 内的 MLD Snooping 版本

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入MLD-Snooping视图	<b>mld-snooping</b>	-
配置指定VLAN内的MLD Snooping的版本	<b>version version-number vlan vlan-list</b>	缺省情况下，MLD Snooping的版本为1

## 2. 在VLAN内配置MLD Snooping版本

表1-6 在 VLAN 内配置 MLD Snooping 版本

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入VLAN视图	<b>vlan vlan-id</b>	-
配置MLD Snooping的版本	<b>mld-snooping version version-number</b>	缺省情况下，MLD Snooping的版本为1



### 说明

当 MLD Snooping 的版本由版本 2 切换到版本 1 时，系统将清除所有通过动态加入的 MLD Snooping 转发表项；对于在版本 2 下通过手工配置而静态加入的 MLD Snooping 转发表项，则分为以下两种情况进行不同的处理：

- 如果配置的仅仅是静态加入 IPv6 组播组，而没有指定 IPv6 组播源，则这些转发表项将不会被清除；
- 如果配置的是指定了 IPv6 组播源的静态加入 IPv6 组播源组，则这些转发表项将会被清除，并且当再次切换回版本 2 时，这些转发表项将被重新恢复。

有关静态加入的详细配置，请参见“[1.4.3 配置静态端口](#)”。

### 1.3.4 配置MLD Snooping转发表项的全局最大数量

用户可以调整 MLD Snooping 转发表项的全局最大数量，当设备上维护的表项数量达到最大数量后，将不再创建新的表项，直至有表项被老化或被手工删除。

表1-7 配置 MLD Snooping 转发表项的全局最大数量

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入MLD-Snooping视图	<b>mld-snooping</b>	-
配置MLD Snooping转发表项的全局最大数量	<b>entry-limit limit</b>	缺省情况下，MLD Snooping转发表项的全局最大数量为4294967295



说明

在配置 MLD Snooping 转发表项的全局最大数量时，如果设备上维护的表项数量已超过配置值，系统不会自动删除任何已存在的表项，也不再继续创建新的表项。在这种情况下，建议用户手工删除多余表项。

## 1.4 配置MLD Snooping端口功能

### 1.4.1 配置准备

在配置 MLD Snooping 端口功能之前，需完成以下任务：

- 在 VLAN 内使能 MLD Snooping

在配置 MLD Snooping 端口功能之前，需准备以下数据：

- 动态路由器端口老化时间
- 动态成员端口老化时间
- IPv6 组播组和 IPv6 组播源的地址

### 1.4.2 配置动态端口老化定时器

对于动态路由器端口，如果在其老化时间内没有收到 MLD 普遍组查询报文或者 IPv6 PIM Hello 报文，二层设备将把该端口从路由器端口列表中删除。

对于动态成员端口，如果在其老化时间内没有收到该 IPv6 组播组的 MLD 成员关系报告报文，二层设备将把该端口从该 IPv6 组播组所对应转发表的出端口列表中删除。

如果 IPv6 组播组成员的变动比较频繁，可以把动态成员端口老化时间设置小一些，反之亦然。

用户既可在 MLD-Snooping 视图下对所有 VLAN 进行全局配置，也可在 VLAN 视图下只对当前 VLAN 进行配置，后者的配置优先级较高。



说明

如果动态路由器端口收到的是 IPv6 PIMv2 Hello 报文，那么该端口的老化时间将由 IPv6 PIMv2 Hello 报文所携带的参数决定，而不受本节配置的影响。

### 1. 全局配置动态端口老化定时器

表1-8 全局配置动态端口老化定时器

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入MLD-Snooping视图	<b>mld-snooping</b>	-
全局配置动态路由器端口老化时间	<b>router-aging-time interval</b>	缺省情况下，动态路由器端口的老化时间为260秒

操作	命令	说明
全局配置动态成员端口老化时间	<b>host-aging-time interval</b>	缺省情况下，动态成员端口的老化时间为260秒

## 2. 在VLAN内配置动态端口老化定时器

表1-9 在 VLAN 内配置动态端口老化定时器

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入VLAN视图	<b>vlan vlan-id</b>	-
在VLAN内配置动态路由器端口老化时间	<b>mld-snooping router-aging-time interval</b>	缺省情况下，动态路由器端口的老化时间为260秒
在VLAN内配置动态成员端口老化时间	<b>mld-snooping host-aging-time interval</b>	缺省情况下，动态成员端口的老化时间为260秒

### 1.4.3 配置静态端口

如果某端口所连接的主机需要固定接收发往某 IPv6 组播组的 IPv6 组播数据，可以配置该端口静态加入该 IPv6 组播组，成为静态成员端口。静态成员端口不会对 MLD 查询器发出的查询报文进行响应；当配置静态成员端口或取消静态成员端口的配置时，端口也不会主动发送 MLD 成员关系报告报文或 MLD 离开组报文。

可以通过将二层设备上的端口配置为静态路由器端口，从而使二层设备上所有收到的 IPv6 组播数据可以通过该端口被转发出去。

表1-10 配置静态端口

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入二层以太网或二层聚合接口视图	<b>interface interface-type interface-number</b>	-
配置静态成员端口	<b>mld-snooping static-group ipv6-group-address [ source-ip ipv6-source-address ] vlan vlan-id</b>	缺省情况下，端口不是静态成员端口
配置静态路由器端口	<b>mld-snooping static-router-port vlan vlan-id</b>	缺省情况下，端口不是静态路由器端口



静态成员端口和静态路由器端口都不会老化，只能通过相应的 **undo** 命令删除。

## 1.4.4 配置模拟主机加入

在二层设备的端口上配置了模拟主机加入后,该模拟主机就可以模仿真实的 IPv6 组播组成员主机,对 MLD 查询器发出的查询报文进行响应,包括:

- 启动模拟主机时,该端口会主动发送一个 MLD 成员关系报告报文。
- 在模拟主机的运行过程中,当收到 MLD 查询报文时,该端口会响应一个 MLD 成员关系报告报文。
- 停止模拟主机时,该端口会发送一个 MLD 离开组报文。



说明

- 与静态成员端口不同,配置了模拟主机加入的端口将作为动态成员端口参与动态成员端口的老化过程。
- 模拟主机所采用的 MLD 版本与 MLD Snooping 的版本一致。

表1-11 配置模拟主机加入

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入二层以太网或二层聚合接口视图	<b>interface</b> <i>interface-type</i> <i>interface-number</i>	-
配置模拟主机加入IPv6组播组或IPv6组播源组	<b>mld-snooping host-join</b> <i>ipv6-group-address</i> [ <b>source-ip</b> <i>ipv6-source-address</i> ] <b>vlan</b> <i>vlan-id</i>	缺省情况下,没有配置模拟主机加入IPv6组播组或IPv6组播源组

## 1.4.5 配置端口快速离开

端口快速离开是指当端口收到主机发来的离开指定 IPv6 组播组的 MLD 离开组报文时,直接将该端口从相应转发表项的出端口列表中删除。此后,当收到针对该 IPv6 组播组的 MLD 特定组查询报文时,二层设备将不再向该端口转发。

对于一个 VLAN,只有当一个端口下只有一个接收者时,才建议配置本功能;否则,当一个端口下有多个接收者时,其中一个接收者的离开会触发该端口的快速离开,从而导致属于同一 IPv6 组播组的其它接收者无法收到 IPv6 组播数据。

用户既可在 MLD-Snooping 视图下对所有端口进行全局配置,也可在接口视图下只对当前端口进行配置,后者的配置优先级较高。

### 1. 全局配置端口快速离开

表1-12 全局配置端口快速离开

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入MLD-Snooping视图	<b>mld-snooping</b>	-

操作	命令	说明
全局使能端口快速离开功能	<b>fast-leave [ vlan <i>vlan-list</i> ]</b>	缺省情况下，端口快速离开功能处于关闭状态

## 2. 在端口上配置端口快速离开

表1-13 在端口上配置端口快速离开

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入二层以太网或二层聚合接口视图	<b>interface <i>interface-type</i> <i>interface-number</i></b>	-
在端口上使能端口快速离开功能	<b>mld-snooping fast-leave [ vlan <i>vlan-list</i> ]</b>	缺省情况下，端口快速离开功能处于关闭状态

## 1.5 配置MLD Snooping查询器

### 1.5.1 配置准备

在配置 MLD Snooping 查询器之前，需完成以下任务：

- 在 VLAN 内使能 MLD Snooping

在配置 MLD Snooping 查询器之前，需准备以下数据：

- MLD 普遍组查询报文的发送间隔
- MLD 特定组查询报文的发送间隔
- MLD 普遍组查询的最大响应时间

### 1.5.2 使能MLD Snooping查询器

在运行了 MLD 的 IPv6 组播网络中，会有一台三层组播设备充当 MLD 查询器，负责发送 MLD 查询报文，使三层组播设备能够在网络层建立并维护 IPv6 组播转发表项，从而在网络层正常转发 IPv6 组播数据。

但是，在一个没有三层组播设备的网络中，由于二层设备并不支持 MLD，因此无法实现 MLD 查询器的相关功能。为了解决这个问题，可以在二层设备上使能 MLD Snooping 查询器，使二层设备能够在数据链路层建立并维护 IPv6 组播转发表项，从而在数据链路层正常转发 IPv6 组播数据。



提示

请避免在运行了 MLD 的网络中配置 MLD Snooping 查询器，因为尽管 MLD Snooping 查询器并不参与 MLD 查询器的选举，但在运行了 MLD 的网络中，配置 MLD Snooping 查询器不但没有实际的意义，反而可能会由于其发送的 MLD 普遍组查询报文的源 IPv6 地址较小而影响 MLD 查询器的选举。有关 MLD 查询器的详细介绍，请参见“IP 组播配置指导”中的“MLD”。

表1-14 使能 MLD Snooping 查询器

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入VLAN视图	<b>vlan <i>vlan-id</i></b>	-
使能MLD Snooping查询器	<b>mld-snooping querier</b>	缺省情况下，MLD Snooping查询器处于关闭状态

### 1.5.3 配置MLD查询和响应

可以根据网络的实际情况来修改 MLD 普遍组查询报文的发送间隔。

在收到 MLD 查询报文（包括普遍组查询和特定组查询）后，主机会为其所加入的每个 IPv6 组播组都启动一个定时器，定时器的值在 0 到最大响应时间（该时间值由主机从所收到的 MLD 查询报文的最大响应时间字段获得）中随机选定，当定时器的值减为 0 时，主机就会向该定时器对应的 IPv6 组播组发送 MLD 成员关系报告报文。

合理配置 MLD 查询的最大响应时间，既可以使主机对 MLD 查询报文做出快速响应，又可以减少由于定时器同时超时，造成大量主机同时发送报告报文而引起的网络拥塞：

- 对于 MLD 普遍组查询报文来说，通过配置 MLD 普遍组查询的最大响应时间来填充其最大响应时间字段；
- 对于 MLD 特定组查询报文来说，所配置的 MLD 特定组查询报文的发送间隔将被填充到其最大响应时间字段。也就是说，MLD 特定组查询的最大响应时间从数值上与 MLD 特定组查询报文的发送间隔相同。

用户既可在 MLD-Snooping 视图下对所有 VLAN 进行全局配置，也可在 VLAN 视图下只对当前 VLAN 进行配置，后者的配置优先级较高。



提示

为 避免对 IPv6 组播组成员的误删，请 确保 MLD 普遍组查询报文的发送间隔大于 MLD 普遍组查询的最大响应时间， 否则 配置虽 能生效但系统会给出提示。

#### 1. 全局配置MLD查询和响应

表1-15 全局配置 MLD 查询和响应

操作	命令	说明
进入系统视图	<b>system-view</b>	-

操作	命令	说明
进入MLD-Snooping视图	<b>mld-snooping</b>	-
全局配置MLD普遍组查询的最大响应时间	<b>max-response-time interval</b>	缺省情况下，MLD普遍组查询的最大响应时间为10秒
全局配置MLD特定组查询报文的发送间隔	<b>last-listener-query-interval interval</b>	缺省情况下，MLD特定组查询报文的发送间隔为1秒

## 2. 在VLAN内配置MLD查询和响应

表1-16 在 VLAN 内配置 MLD 查询和响应

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入VLAN视图	<b>vlan vlan-id</b>	-
在VLAN内配置MLD普遍组查询报文的发送间隔	<b>mld-snooping query-interval interval</b>	缺省情况下，MLD普遍组查询报文的发送间隔为125秒
在VLAN内配置MLD普遍组查询的最大响应时间	<b>mld-snooping max-response-time interval</b>	缺省情况下，MLD普遍组查询的最大响应时间为10秒
在VLAN内配置MLD特定组查询报文的发送间隔	<b>mld-snooping last-listener-query-interval interval</b>	缺省情况下，MLD特定组查询报文的发送间隔为1秒

## 1.6 调整MLD报文

### 1.6.1 配置准备

在调整 MLD 报文之前，需完成以下任务：

- 在 VLAN 内使能 MLD Snooping

在调整 MLD 报文之前，需准备以下数据：

- MLD 普遍组查询报文的源 IPv6 地址
- MLD 特定组查询报文的源 IPv6 地址
- MLD 成员关系报告报文的源 IPv6 地址
- MLD 离开组报文的源 IPv6 地址

### 1.6.2 配置MLD报文的源IPv6地址

用户可以通过本配置改变 MLD Snooping 查询器发送的 MLD 查询报文的源 IPv6 地址。

用户也可以通过本配置改变模拟主机发送的 MLD 成员关系报告报文或 MLD 离开组报文的源 IPv6 地址。



提示

MLD 查询报文的源 IPv6 地址的改变可能会影响网段内 MLD 查询器的选举。

表1-17 配置 MLD 报文的源 IPv6 地址

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入VLAN视图	<b>vlan</b> <i>vlan-id</i>	-
配置MLD普遍组查询报文的源IPv6地址	<b>mld-snooping general-query source-ip</b> <i>ipv6-address</i>	缺省情况下，MLD普遍组查询报文的源IPv6地址为当前VLAN接口的IPv6链路本地地址；若当前VLAN接口没有IPv6链路本地地址，则采用FE80::02FF:FFFF:FE00:0001
配置MLD特定组查询报文的源IPv6地址	<b>mld-snooping special-query source-ip</b> <i>ipv6-address</i>	缺省情况下，如果收到过MLD普遍组查询报文，则以其源IPv6地址作为MLD特定组查询报文的源IPv6地址；否则，采用当前VLAN接口的IPv6链路本地地址；若当前VLAN接口没有IPv6链路本地地址，则采用FE80::02FF:FFFF:FE00:0001
配置MLD成员关系报告报文的源IPv6地址	<b>mld-snooping report source-ip</b> <i>ipv6-address</i>	缺省情况下，MLD成员关系报告报文的源IPv6地址为当前VLAN接口的IPv6链路本地地址；若当前VLAN接口没有IPv6链路本地地址，则采用FE80::02FF:FFFF:FE00:0001
配置MLD离开组报文的源IPv6地址	<b>mld-snooping done source-ip</b> <i>ipv6-address</i>	缺省情况下，MLD离开组报文的源IPv6地址为当前VLAN接口的IPv6链路本地地址；若当前VLAN接口没有IPv6链路本地地址，则采用FE80::02FF:FFFF:FE00:0001

## 1.7 配置MLD Snooping策略

### 1.7.1 配置准备

在配置 MLD Snooping 策略之前，需完成以下任务：

- 在 VLAN 内使能 MLD Snooping

在配置 MLD Snooping 策略之前，需准备以下数据：

- IPv6 组播组过滤的 ACL 规则
- 端口加入的 IPv6 组播组最大数量

### 1.7.2 配置IPv6 组播组过滤器



提示

本配置只对动态组播组有效，对静态组播组无效。

在使能了 MLD Snooping 的交换机上，通过配置 IPv6 组播组过滤器，可以限制用户对组播节目的点播。



在实际应用中，当用户点播某个组播节目时，主机会发起一个 MLD 成员关系报告报文，该报文到达交换机后，进行 ACL 检查：如果该接收端口可以加入这个 IPv6 组播组，则将其列入到 MLD Snooping 转发表中；否则交换机就丢弃该报文。这样，未通过 ACL 检查的 IPv6 组播数据就不会送到该端口，从而达到控制用户点播组播节目的目的。

用户既可在 MLD-Snooping 视图下对所有端口进行全局配置，也可在接口视图下只对当前端口进行配置，后者的配置优先级较高。

### 1. 全局配置IPv6 组播组过滤器

表1-18 全局配置 IPv6 组播组过滤器

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入MLD-Snooping视图	<b>mld-snooping</b>	-
全局配置IPv6组播组过滤器	<b>group-policy acl6-number [ vlan vlan-list ]</b>	缺省情况下，没有配置IPv6组播组过滤器，即主机可以加入任意合法的IPv6组播组

### 2. 在端口上配置IPv6 组播组过滤器

表1-19 在端口上配置 IPv6 组播组过滤器

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入二层以太网或二层聚合接口视图	<b>interface interface-type interface-number</b>	-
在端口上配置IPv6组播组过滤器	<b>mld-snooping group-policy acl6-number [ vlan vlan-list ]</b>	缺省情况下，没有配置IPv6组播组过滤器，即主机可以加入任意合法的IPv6组播组

## 1.7.3 配置丢弃未知IPv6 组播数据报文

未知 IPv6 组播数据报文是指在 MLD Snooping 转发表中不存在对应转发表项的那些 IPv6 组播数据报文：

- 当使能了丢弃未知 IPv6 组播数据报文功能时，二层设备仅向未知 IPv6 组播数据报文所属的 VLAN 内的其它路由器端口转发该报文，不在 VLAN 内广播；
- 当关闭了丢弃未知 IPv6 组播数据报文功能时，二层设备将在未知 IPv6 组播数据报文所属的 VLAN 内广播该报文。

表1-20 在 VLAN 内配置丢弃未知 IPv6 组播数据报文

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入VLAN视图	<b>vlan vlan-id</b>	-

操作	命令	说明
在VLAN内使能丢弃未知IPv6组播数据报文功能	<b>mld-snooping drop-unknown</b>	缺省情况下，丢弃未知IPv6组播数据报文功能处于关闭状态，即对未知IPv6组播数据报文进行广播

#### 1.7.4 配置MLD成员关系报告报文抑制

当二层设备收到来自某 IPv6 组播组成员的 MLD 成员关系报告报文时，会将该报文转发给与其直连的三层设备。这样，当二层设备上存在属于某 IPv6 组播组的多个成员时，与其直连的三层设备会收到这些成员发送的相同 MLD 成员关系报告报文。

当使能了 MLD 成员关系报告报文抑制功能后，在一个查询间隔内二层设备只会把收到的某 IPv6 组播组内的第一个 MLD 成员关系报告报文转发给三层设备，而不继续向三层设备转发来自同一 IPv6 组播组的其它 MLD 成员关系报告报文，这样可以减少网络中的报文数量。

表1-21 配置 MLD 成员关系报告报文抑制

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入MLD-Snooping视图	<b>mld-snooping</b>	-
使能MLD成员关系报告报文抑制功能	<b>report-aggregation</b>	缺省情况下，MLD 成员关系报告报文抑制功能处于使能状态

#### 1.7.5 配置端口加入的IPv6组播组最大数量



提示

本配置只对动态组播组有效，对静态组播组无效。

通过配置端口加入的 IPv6 组播组的最大数量，可以限制用户点播组播节目的数量，从而控制了端口上的数据流量。

表1-22 配置端口加入的 IPv6 组播组最大数量

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入二层以太网或二层聚合接口视图	<b>interface interface-type interface-number</b>	-
配置端口加入的IPv6组播组最大数量	<b>mld-snooping group-limit limit [ vlan vlan-list ]</b>	缺省情况下，端口加入的IPv6组播组最大数量为4294967295



说明

在配置端口加入的 IPv6 组播组最大数量时，如果当前端口上的 IPv6 组播组数量已超过配置值，系统将把该端口相关的所有转发表项从 MLD Snooping 转发表中删除，该端口下的主机都需要重新加入 IPv6 组播组，直至该端口上的 IPv6 组播组数量达到限制值为止。

## 1.7.6 配置IPv6 组播组替换功能



提示

本配置只对动态组播组有效，对静态组播组无效。

由于某些特殊的原因，当前二层设备或端口上通过的 IPv6 组播组数目有可能会超过二层设备或该端口的限定；另外，在某些特定的应用中，二层设备上新加入的 IPv6 组播组需要自动替换已存在的 IPv6 组播组（一个典型的应用就是“频道切换”，即用户通过加入一个新的 IPv6 组播组就能完成离开原 IPv6 组播组并切换到新 IPv6 组播组的动作）。

针对以上情况，可以在二层设备或者某些端口上使能 IPv6 组播组替换功能。当二层设备或端口上加入的 IPv6 组播组数量已达到限定值时：

- 若使能了 IPv6 组播组替换功能，则新加入的 IPv6 组播组会自动替代已存在的 IPv6 组播组，替代规则是替代 IPv6 地址最小的 IPv6 组播组；
- 若没有使能 IPv6 组播组替换功能，则自动丢弃新的 MLD 成员关系报告报文。

用户既可在 MLD-Snooping 视图下对所有端口进行全局配置，也可在接口视图下只对当前端口进行配置，后者的配置优先级较高。

### 1. 全局配置IPv6 组播组替换功能

表1-23 全局配置 IPv6 组播组替换功能

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入MLD-Snooping视图	<b>mld-snooping</b>	-
全局使能IPv6组播组替换功能	<b>overflow-replace [ vlan <i>vlan-list</i> ]</b>	缺省情况下，IPv6组播组替换功能处于关闭状态

### 2. 在端口上配置IPv6 组播组替换功能

表1-24 在端口上配置 IPv6 组播组替换功能

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入二层以太网或二层聚合接口视图	<b>interface <i>interface-type</i> <i>interface-number</i></b>	-

操作	命令	说明
在端口上使能IPv6组播组替换功能	<b>mld-snooping overflow-replace [ vlan <i>vlan-list</i> ]</b>	缺省情况下，IPv6组播组替换功能处于关闭状态

## 1.8 MLD Snooping显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 MLD Snooping 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 MLD Snooping 的信息。

表1-25 MLD Snooping 显示和维护

操作	命令
显示IPv6二层组播的IP组播组信息（独立运行模式）	<b>display ipv6 I2-multicast ip [ group <i>ipv6-group-address</i>   source <i>ipv6-source-address</i> ] * [ vlan <i>vlan-id</i> ] [ slot <i>slot-number</i> ]</b>
显示IPv6二层组播的IP组播组信息（IRF模式）	<b>display ipv6 I2-multicast ip [ group <i>ipv6-group-address</i>   source <i>ipv6-source-address</i> ] * [ vlan <i>vlan-id</i> ] [ chassis <i>chassis-number</i> slot <i>slot-number</i> ]</b>
显示IPv6二层组播的IP转发表信息（独立运行模式）	<b>display ipv6 I2-multicast ip forwarding [ group <i>ipv6-group-address</i>   source <i>ipv6-source-address</i> ] * [ vlan <i>vlan-id</i> ] [ slot <i>slot-number</i> ]</b>
显示IPv6二层组播的IP转发表信息（IRF模式）	<b>display ipv6 I2-multicast ip forwarding [ group <i>ipv6-group-address</i>   source <i>ipv6-source-address</i> ] * [ vlan <i>vlan-id</i> ] [ chassis <i>chassis-number</i> slot <i>slot-number</i> ]</b>
显示IPv6二层组播的MAC组播组信息（独立运行模式）	<b>display ipv6 I2-multicast mac [ <i>mac-address</i> ] [ vlan <i>vlan-id</i> ] [ slot <i>slot-number</i> ]</b>
显示IPv6二层组播的MAC组播组信息（IRF模式）	<b>display ipv6 I2-multicast mac [ <i>mac-address</i> ] [ vlan <i>vlan-id</i> ] [ chassis <i>chassis-number</i> slot <i>slot-number</i> ]</b>
显示IPv6二层组播的MAC转发表信息（独立运行模式）	<b>display ipv6 I2-multicast mac forwarding [ <i>mac-address</i> ] [ vlan <i>vlan-id</i> ] [ slot <i>slot-number</i> ]</b>
显示IPv6二层组播的MAC转发表信息（IRF模式）	<b>display ipv6 I2-multicast mac forwarding [ <i>mac-address</i> ] [ vlan <i>vlan-id</i> ] [ chassis <i>chassis-number</i> slot <i>slot-number</i> ]</b>
显示MLD Snooping的状态信息	<b>display mld-snooping [ global   vlan <i>vlan-id</i> ]</b>
显示IPv6动态组播组的MLD Snooping转发表项信息（独立运行模式）	<b>display mld-snooping group [ <i>ipv6-group-address</i>   <i>ipv6-source-address</i> ] * [ vlan <i>vlan-id</i> ] [ verbose ] [ slot <i>slot-number</i> ]</b>
显示IPv6动态组播组的MLD Snooping转发表项信息（IRF模式）	<b>display mld-snooping group [ <i>ipv6-group-address</i>   <i>ipv6-source-address</i> ] * [ vlan <i>vlan-id</i> ] [ verbose ] [ chassis <i>chassis-number</i> slot <i>slot-number</i> ]</b>
显示IPv6静态组播组的MLD Snooping转发表项信息（独立运行模式）	<b>display mld-snooping static-group [ <i>ipv6-group-address</i>   <i>ipv6-source-address</i> ] * [ vlan <i>vlan-id</i> ] [ verbose ] [ slot <i>slot-number</i> ]</b>
显示IPv6静态组播组的MLD Snooping转发表项信息（IRF模式）	<b>display mld-snooping static-group [ <i>ipv6-group-address</i>   <i>ipv6-source-address</i> ] * [ vlan <i>vlan-id</i> ] [ verbose ] [ chassis <i>chassis-number</i> slot <i>slot-number</i> ]</b>
显示IPv6动态路由器端口的信息（独立运行模式）	<b>display mld-snooping router-port [ vlan <i>vlan-id</i> ] [ slot <i>slot-number</i> ]</b>

操作	命令
显示IPv6动态路由器端口的信息（IRF模式）	<b>display mld-snooping router-port</b> [ vlan <i>vlan-id</i> ] [ chassis <i>chassis-number</i> slot <i>slot-number</i> ]
显示IPv6静态路由器端口的信息（独立运行模式）	<b>display mld-snooping static-router-port</b> [ vlan <i>vlan-id</i> ] [ slot <i>slot-number</i> ]
显示IPv6静态路由器端口的信息（IRF模式）	<b>display mld-snooping static-router-port</b> [ vlan <i>vlan-id</i> ] [ chassis <i>chassis-number</i> slot <i>slot-number</i> ]
显示MLD Snooping监听到的MLD报文统计信息	<b>display mld-snooping statistics</b>
清除IPv6动态组播组的MLD Snooping转发表项信息	<b>reset mld-snooping group</b> { <i>ipv6-group-address</i> [ <i>ipv6-source-address</i> ]   all } [ vlan <i>vlan-id</i> ]
清除IPv6动态路由器端口的信息	<b>reset mld-snooping router-port</b> { all   vlan <i>vlan-id</i> }
清除MLD Snooping监听到的MLD报文统计信息	<b>reset mld-snooping statistics</b>

## 1.9 MLD Snooping典型配置举例



说明

缺省情况下，以太网接口、VLAN接口及聚合接口处于DOWN状态。如果要使这些接口能够正常工作，请先使用undo shutdown命令使接口处于UP状态。

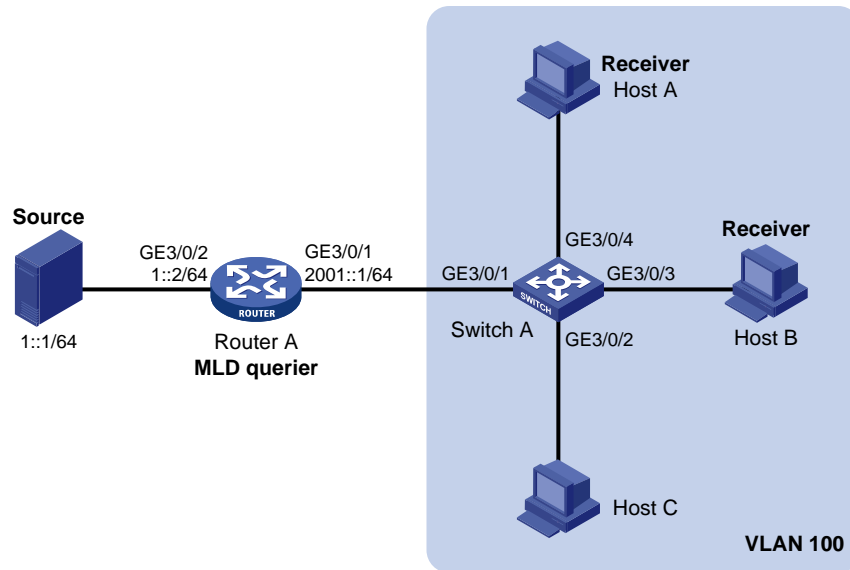
### 1.9.1 IPv6组策略及模拟主机加入配置举例

#### 1. 组网需求

- 如图 1-3 所示，Router A通过GigabitEthernet3/0/2 接口连接IPv6组播源（Source），通过GigabitEthernet3/0/1 接口连接Switch A；Router A上运行MLDv1，Switch A上运行版本 1 的MLD Snooping，并由Router A充当MLD查询器。
- 通过配置，使 Host A 和 Host B 能且只能接收发往 IPv6 组播组 FF1E::101 的 IPv6 组播数据，并且当 Host A 和 Host B 即使发生意外而临时中断接收 IPv6 组播数据时，发往 IPv6 组播组 FF1E::101 的 IPv6 组播数据也能不间断地通过 Switch A 的接口 GigabitEthernet3/0/3 和 GigabitEthernet3/0/4 转发出去；同时，使 Switch A 将收到的未知 IPv6 组播数据直接丢弃，避免在其所属的 VLAN 100 内广播。

## 2. 组网图

图1-3 IPv6 组策略及模拟主机加入配置组网图



## 3. 配置步骤

### (1) 配置 IPv6 地址

请按照 [图 1-3](#) 配置各接口的IPv6 地址和前缀长度，具体配置过程略。

### (2) 配置 Router A

# 使能 IPv6 组播路由，在接口 GigabitEthernet3/0/2 上使能 IPv6 PIM-DM，并在接口 GigabitEthernet3/0/1 上使能 MLD。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 3/0/1
[RouterA-GigabitEthernet3/0/1] mld enable
[RouterA-GigabitEthernet3/0/1] quit
[RouterA] interface gigabitethernet 3/0/2
[RouterA-GigabitEthernet3/0/2] ipv6 pim dm
[RouterA-GigabitEthernet3/0/2] quit
```

### (3) 配置 Switch A

# 全局使能 MLD Snooping。

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet3/0/1 到 GigabitEthernet3/0/4 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并使能丢弃未知 IPv6 组播数据报文功能。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 3/0/1 to gigabitethernet 3/0/4
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping drop-unknown
```

```
[SwitchA-vlan100] quit
# 配置 IPv6 组播组过滤器，以限定 VLAN 100 内的主机只能加入 IPv6 组播组 FF1E::101。
[SwitchA] acl ipv6 number 2001
[SwitchA-acl6-basic-2001] rule permit source ff1e::101 128
[SwitchA-acl6-basic-2001] quit
[SwitchA] mld-snooping
[SwitchA-mld-snooping] group-policy 2001 vlan 100
[SwitchA-mld-snooping] quit
# 在 GigabitEthernet3/0/1 和 GigabitEthernet3/0/4 上分别配置模拟主机加入 IPv6 组播组 FF1E::101。
[SwitchA] interface gigabitethernet3/0/1
[SwitchA-GigabitEthernet3/0/1] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet3/0/1] quit
[SwitchA] interface gigabitethernet3/0/4
[SwitchA-GigabitEthernet3/0/4] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet3/0/4] quit
```

#### 4. 验证配置

假设 IPv6 组播源分别向 IPv6 组播组 FF1E::101 和 FF1E::202 发送的 IPv6 组播数据，Host A 和 Host B 也都申请加入这两个 IPv6 组播组。

# 显示 Switch A 上 VLAN 100 内 IPv6 动态组播组的 MLD Snooping 转发表项信息。

```
[SwitchA] display mld-snooping group vlan 100
Total 1 entries.
```

```
VLAN 100: Total 1 entries.
(::, FF1E::101)
Host slots (1 in total):
  3
Host ports (2 in total):
  GE3/0/3      (00:03:23)
  GE3/0/4      (00:04:10)
```

由此可见，Host A 和 Host B 所在的端口 GigabitEthernet3/0/4 和 GigabitEthernet3/0/3 均已加入 IPv6 组播组 FF1E::101，但都未加入 IPv6 组播组 FF1E::202，这表明 IPv6 组播组过滤器已生效。

## 1.9.2 静态端口配置举例

### 1. 组网需求

- 如 [图 1-4](#) 所示，Router A 通过 GigabitEthernet3/0/2 接口连接 IPv6 组播源（Source），通过 GigabitEthernet3/0/1 接口连接 Switch A；Router A 上运行 MLDv1，Switch A、Switch B 和 Switch C 上运行版本 1 的 MLD Snooping，并由 Router A 充当 MLD 查询器。
- Host A 和 Host C 均为 IPv6 组播组 FF1E::101 的固定接收者（Receiver），通过将 Switch C 上的端口 GigabitEthernet3/0/3 和 GigabitEthernet3/0/5 配置为 IPv6 组播组 FF1E::101 的静态成员端口，可以增强 IPv6 组播数据在传输过程中的可靠性。
- 假设由于受 STP 等链路层协议的影响，为了避免出现环路，Switch A—Switch C 的转发路径在正常情况下是阻断的，IPv6 组播数据只能通过 Switch A—Switch B—Switch C 的路径传递给连接在 Switch C 上的接收者；要求通过将 Switch A 的端口 GigabitEthernet3/0/3 配置为静

态路由器端口，以保证当 Switch A—Switch B—Switch C 的路径出现阻断时，IPv6 组播数据可以几乎不间断地通过 Switch A—Switch C 的新路径传递给接收者。

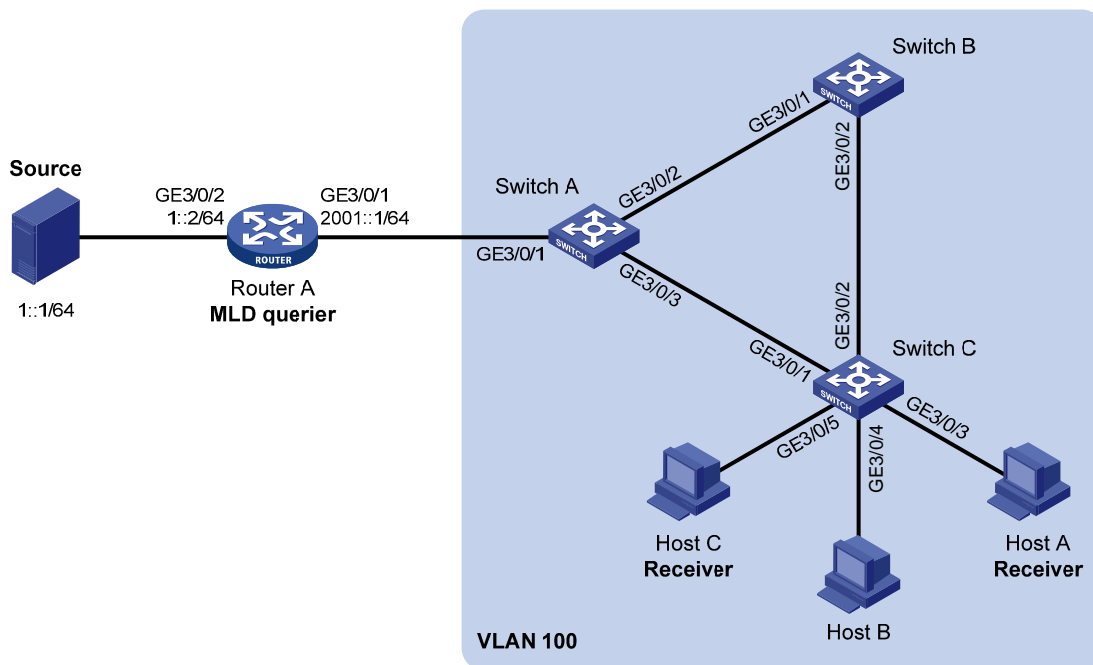
### 说明

如果没有配置静态路由器端口，那么当 Switch A—Switch B—Switch C 的路径出现阻断时，至少需要等待一个 MLD 查询和响应周期完成后，IPv6 组播数据才能通过 Switch A—Switch C 的新路径传递给接收者，IPv6 组播数据的传输在这个过程中将中断。

有关 STP（Spanning Tree Protocol，生成树协议）的详细介绍，请参见“二层技术-以太网交换配置指导”中的“生成树”。

## 2. 组网图

图1-4 静态端口配置组网图



## 3. 配置步骤

### (1) 配置 IPv6 地址

请按照 [图 1-4](#) 配置各接口的 IPv6 地址和前缀长度，具体配置过程略。

### (2) 配置 Router A

# 使能 IPv6 组播路由，在接口 GigabitEthernet3/0/2 上使能 IPv6 PIM-DM，并在接口 GigabitEthernet3/0/1 上使能 MLD。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 3/0/1
[RouterA-GigabitEthernet3/0/1] mld enable
[RouterA-GigabitEthernet3/0/1] quit
```



```
[RouterA] interface gigabitethernet 3/0/2
[RouterA-GigabitEthernet3/0/2] ipv6 pim dm
[RouterA-GigabitEthernet3/0/2] quit
```

### (3) 配置 Switch A

# 全局使能 MLD Snooping。

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet3/0/1 到 GigabitEthernet3/0/3 添加到该 VLAN 中，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 3/0/1 to gigabitethernet 3/0/3
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] quit
```

# 把 GigabitEthernet3/0/3 配置为静态路由器端口。

```
[SwitchA] interface gigabitethernet 3/0/3
[SwitchA-GigabitEthernet3/0/3] mld-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet3/0/3] quit
```

### (4) 配置 Switch B

# 全局使能 MLD Snooping。

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet3/0/1 和 GigabitEthernet3/0/2 添加到该 VLAN 中，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 3/0/1 gigabitethernet 3/0/2
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] quit
```

### (5) 配置 Switch C

# 全局使能 MLD Snooping。

```
<SwitchC> system-view
[SwitchC] mld-snooping
[SwitchC-mld-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet3/0/1 到 GigabitEthernet3/0/5 添加到该 VLAN 中，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 3/0/1 to gigabitethernet 3/0/5
[SwitchC-vlan100] mld-snooping enable
[SwitchC-vlan100] quit
```

# 分别在端口 GigabitEthernet3/0/3 和 GigabitEthernet3/0/5 上配置静态加入 IPv6 组播组 FF1E::101。

```
[SwitchC] interface gigabitethernet 3/0/3
[SwitchC-GigabitEthernet3/0/3] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet3/0/3] quit
[SwitchC] interface gigabitethernet 3/0/5
```

```
[SwitchC-GigabitEthernet3/0/5] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet3/0/5] quit
```

#### 4. 验证配置

# 显示 Switch A 上 VLAN 100 内静态路由器端口的信息。

```
[SwitchA] display mld-snooping static-router-port vlan 100
VLAN 100:
  Router slots (1 in total):
    3
  Router ports (1 in total):
    GE3/0/3
```

由此可见，Switch A 上的端口 GigabitEthernet3/0/3 已经成为了静态路由器端口。

# 显示 Switch C 上 VLAN 100 内 IPv6 静态组播组的 MLD Snooping 转发表项信息。

```
[SwitchC] display mld-snooping static-group vlan 100
Total 1 entries.
```

```
VLAN 100: Total 1 entries.
(::, FF1E::101)
  Host slots (1 in total):
    3
  Host ports (2 in total):
    GE3/0/3
    GE3/0/5
```

由此可见，Switch C 上的端口 GigabitEthernet3/0/3 和 GigabitEthernet3/0/5 已经成为了 IPv6 组播组 FF1E::101 的静态成员端口。

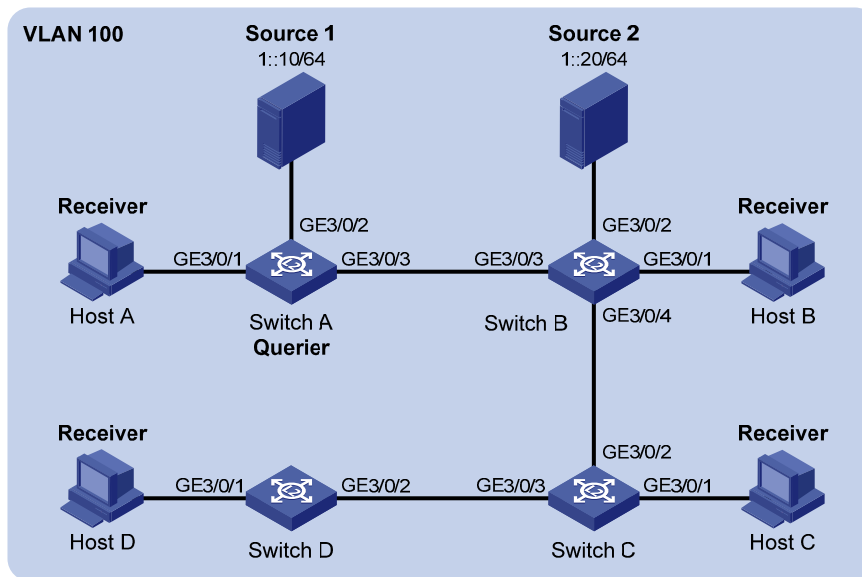
### 1.9.3 MLD Snooping 查询器配置举例

#### 1. 组网需求

- 如 [图 1-5](#) 所示，在一个没有三层设备的纯二层网络环境中，IPv6 组播源 Source 1 和 Source 2 分别向 IPv6 组播组 FF1E::101 和 FF1E::102 发送 IPv6 组播数据，Host A 和 Host C 是 IPv6 组播组 FF1E::101 的接收者（Receiver），Host B 和 Host D 则是 IPv6 组播组 FF1E::102 的接收者；所有接收者均使用 MLDv1，所有交换机上都运行版本 1 的 MLD Snooping，并选择距 IPv6 组播源最近的 Switch A 来充当 MLD Snooping 查询器。
- 为防止交换机在没有二层 IPv6 组播转发表项时将 IPv6 组播数据在 VLAN 内广播，在所有交换机上都使能丢弃未知 IPv6 组播数据报文功能。

## 2. 组网图

图1-5 MLD Snooping 查询器配置组网图



## 3. 配置步骤

### (1) 配置 Switch A

# 全局使能 MLD Snooping。

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet3/0/1 到 GigabitEthernet3/0/3 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并使能丢弃未知 IPv6 组播数据报文功能。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitEthernet 3/0/1 to gigabitEthernet 3/0/3
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping drop-unknown
```

# 在 VLAN 100 内使能 MLD Snooping 查询器。

```
[SwitchA-vlan100] mld-snooping querier
[SwitchA-vlan100] quit
```

### (2) 配置 Switch B

# 全局使能 MLD Snooping。

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet3/0/1 到 GigabitEthernet3/0/4 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并使能丢弃未知 IPv6 组播数据报文功能。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitEthernet 3/0/1 to gigabitEthernet 3/0/4
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] mld-snooping drop-unknown
```

```
[SwitchB-vlan100] quit
```

### (3) 配置 Switch C

# 全局使能 MLD Snooping。

```
<SwitchC> system-view
```

```
[SwitchC] mld-snooping
```

```
[SwitchC-mld-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet3/0/1 到 GigabitEthernet3/0/3 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并使能丢弃未知 IPv6 组播数据报文功能。

```
[SwitchC] vlan 100
```

```
[SwitchC-vlan100] port gigabitEthernet 3/0/1 to gigabitEthernet 3/0/3
```

```
[SwitchC-vlan100] mld-snooping enable
```

```
[SwitchC-vlan100] mld-snooping drop-unknown
```

```
[SwitchC-vlan100] quit
```

### (4) 配置 Switch D

# 全局使能 MLD Snooping。

```
<SwitchD> system-view
```

```
[SwitchD] mld-snooping
```

```
[SwitchD-mld-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet3/0/1 到 GigabitEthernet3/0/2 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并使能丢弃未知 IPv6 组播数据报文功能。

```
[SwitchD] vlan 100
```

```
[SwitchD-vlan100] port gigabitEthernet 3/0/1 to gigabitEthernet 3/0/2
```

```
[SwitchD-vlan100] mld-snooping enable
```

```
[SwitchD-vlan100] mld-snooping drop-unknown
```

```
[SwitchD-vlan100] quit
```

## 4. 验证配置

当 MLD Snooping 查询器开始工作之后，除查询器以外的所有交换机都能收到 MLD 普遍组查询报文。

# 显示 Switch B 上收到的 MLD 报文的统计信息。

```
[SwitchB] display mld-snooping statistics
```

```
Received MLD general queries: 3
```

```
Received MLDv1 specific queries: 0
```

```
Received MLDv1 reports: 12
```

```
Received MLD dones: 0
```

```
Sent MLDv1 specific queries: 0
```

```
Received MLDv2 reports: 0
```

```
Received MLDv2 reports with right and wrong records: 0
```

```
Received MLDv2 specific queries: 0
```

```
Received MLDv2 specific sg queries: 0
```

```
Sent MLDv2 specific queries: 0
```

```
Sent MLDv2 specific sg queries: 0
```

```
Received error MLD messages: 0
```

## 1.10 常见配置错误举例

### 1.10.1 二层设备不能实现二层组播

#### 1. 故障现象

二层设备不能实现 MLD snooping 二层组播功能。

#### 2. 故障分析

MLD Snooping 没有使能。

#### 3. 处理过程

- (1) 使用 **display mld-snooping** 命令查看 MLD Snooping 的运行状态。
- (2) 如果是没有使能 MLD Snooping，则需先在系统视图下使用 **mld-snooping** 命令全局使能 MLD Snooping，然后在 VLAN 视图下使用 **mld-snooping enable** 命令使能 VLAN 内的 MLD Snooping。
- (3) 如果只是没有在相应 VLAN 下使能 MLD Snooping，则只需在 VLAN 视图下使用 **mld-snooping enable** 命令使能 VLAN 内的 MLD Snooping。

### 1.10.2 配置的IPv6 组播组策略不生效

#### 1. 故障现象

配置了 IPv6 组播组策略，只允许主机加入某些特定的 IPv6 组播组，但主机仍然可以收到发往其它 IPv6 组播组的 IPv6 组播数据。

#### 2. 故障分析

- IPv6 ACL 规则配置不正确；
- IPv6 组播组策略应用不正确；
- 没有使能丢弃未知 IPv6 组播数据报文的功能，使得属于过滤策略之外的 IPv6 组播数据报文（即未知 IPv6 组播数据报文）被广播。

#### 3. 处理过程

- (1) 使用 **display acl ipv6** 命令查看所配置的 IPv6 ACL 规则，检查其是否与所要实现的 IPv6 组播组过滤策略相符合。
- (2) 在 MLD-Snooping 视图或相应的接口视图下使用 **display this** 命令查看是否应用了正确的 IPv6 组播组策略。如果没有，则使用 **group-policy** 或 **mld-snooping group-policy** 命令应用正确的 IPv6 组播组策略。
- (3) 使用 **display mld-snooping** 命令查看是否已使能丢弃未知 IPv6 组播数据报文的功能。如果没有使能，则使用 **mld-snooping drop-unknown** 命令使能丢弃未知 IPv6 组播数据报文功能。