H3C 无线接入点

IP 组播配置指导

新华三技术有限公司
http://www.h3c.com

资料版本：6W106-20170701
产品版本：R1508P11

H3C、H3C、H3CS、H3CIE、H3CNE、Aolynk、Aolynk、H^{3}Care、H3care、IRF、NetPilot、Netflow、SecEngine、SecPath、SecCenter、SecBlade、Comware、ITCMM、HUASAN、华三均为新华三技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前 言

本配置指导介绍了 H3C 无线接入点各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。

说明

手册中设备的接口类型、显示信息与设备型号和配置信息相关，本手册致力于提供全面、准确的显示信息，但实际使用中还请以设备的实际情况为准。

前言部分包含如下内容：

1.1 读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

1.2 本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。

	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

1.3 资料获取方式

您可以通过H3C网站（www.h3c.com）获取最新的产品资料：

- 获取安装类、配置类或维护类等产品资料
  http://www.h3c.com/cn/Technical_Documents
- 获取版本说明书等与软件版本配套的资料
  http://www.h3c.com/cn/Software_Download

1.4 技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com

1.5 资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 IGMP Snooping

说明

本章所指的路由器代表了一般意义下的路由设备，以及配置了路由功能的无线接入点设备。为提高可读性，在手册的描述中将不另行说明。

1.1 IGMP Snooping简介

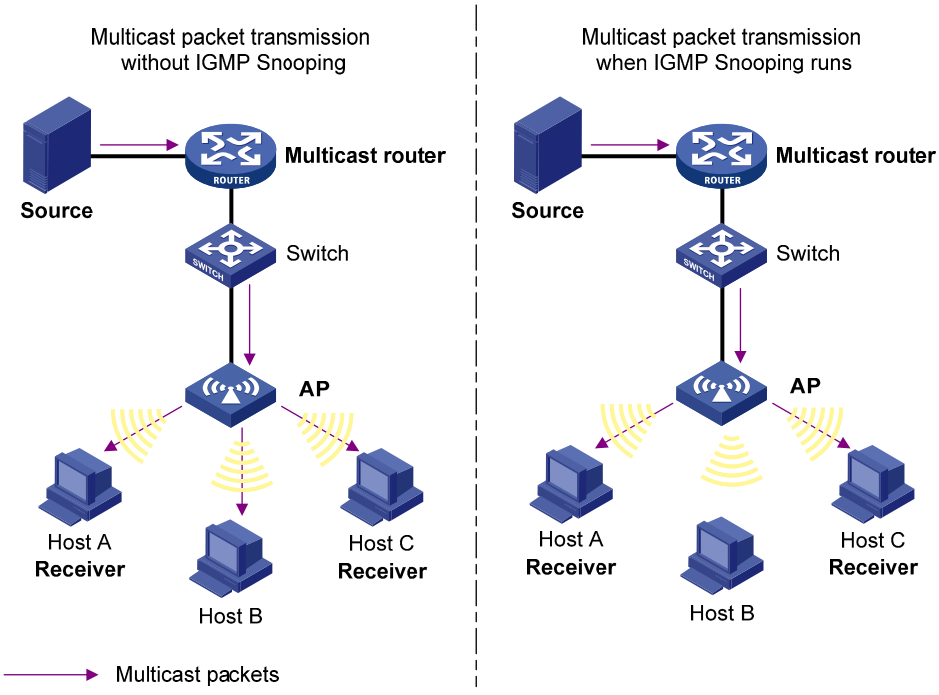
IGMP Snooping 是 Internet Group Management Protocol Snooping（互联网组管理协议窥探）的简称，它是运行在二层设备上的组播约束机制，用于管理和控制组播组。

1.1.1 IGMP Snooping原理

运行 IGMP Snooping 的二层设备通过对收到的 IGMP 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组播数据。

如 图 1-1 所示，当二层设备没有运行IGMP Snooping时，组播数据在二层网络中被广播；当二层设备运行了IGMP Snooping后，已知组播组的组播数据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 IGMP Snooping 前后的对比



IGMP 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：

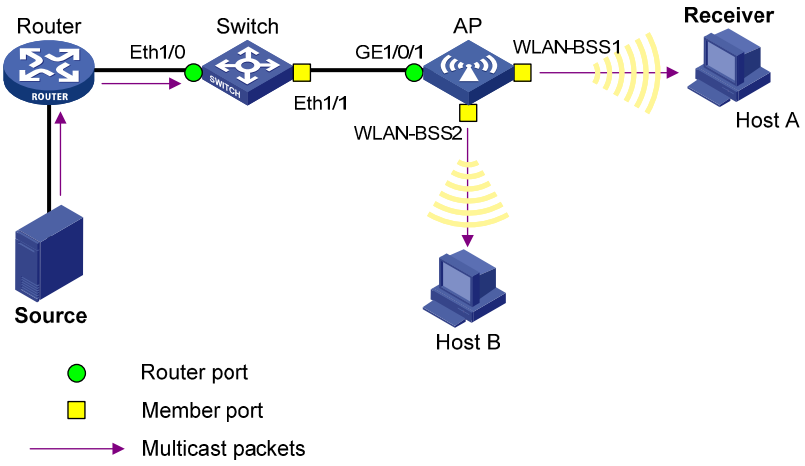
- 减少了二层网络中的广播报文，节约了网络带宽；
- 增强了组播信息的安全性；
- 为实现对每台主机的单独计费带来了方便。

1.1.2 IGMP Snooping基本概念

1. IGMP Snooping相关端口

如 图 1-2 所示，Router A连接组播源，在Switch和AP上分别运行IGMP Snooping，Host A和Host B为接收者主机（即组播组成员）。

图1-2 IGMP Snooping 相关端口



结合 图 1-2，介绍一下IGMP Snooping相关的端口概念：

- 路由器端口（Router Port）：交换机或 AP 上朝向三层组播设备（DR 或 IGMP 查询器）一侧的端口，如 Switch 的 Ethernet1/0 端口和 AP 的 GigabitEthernet1/0/1 端口。交换机和 AP 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）：又称组播组成员端口，表示交换机或 AP 上朝向组播组成员一侧的端口，如 Switch 的 Ethernet1/1 端口，以及 AP 的 WLAN-BSS1 和 WLAN-BSS2 端口。交换机或 AP 将本设备上的所有成员端口都记录在 IGMP Snooping 转发表中。

说明

- 本文中提到的路由器端口都是指交换机或 AP 上朝向组播路由器的端口，而不是指路由器上的端口。
- 如不特别指明，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 IGMP Snooping 的交换机上或 AP，所有收到源地址不为 0.0.0.0 的 IGMP 普遍组查询报文的端口都将被视为动态路由器端口。

---

2. IGMP Snooping动态端口老化定时器

表1-1 IGMP 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 AP 的动作
动态路由器端口老化定时器	AP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0.0.0.0的IGMP普遍组查询报文或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组播组时，AP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	IGMP成员关系报告报文	将该端口从IGMP Snooping转发表中删除

说明

IGMP 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 IGMP Snooping工作机制

运行了 IGMP Snooping 的 AP 对不同 IGMP 动作的具体处理方式如下：

注意

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

IGMP 查询器定期向本地网段内的所有主机与路由器（224.0.0.1）发送 IGMP 普遍组查询报文，以查询该网段有哪些组播组的成员。

在收到 IGMP 普遍组查询报文时，AP 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 IGMP 查询器发送 IGMP 成员关系报告报文：

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

在收到 IGMP 成员关系报告报文时，AP 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。


说明

AP 不会将 IGMP 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 IGMP 成员关系报告抑制机制，如果非路由器端口下还有该组播组的成员主机，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 AP 无法获知这些端口下还有该组播组的成员主机。有关主机上的 IGMP 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“IGMP”。

3. 离开组播组

运行 IGMPv1 的主机离开组播组时不会发送 IGMP 离开组报文，因此 AP 无法立即获知主机离开的信息。但是，由于主机离开组播组后不会再发送 IGMP 成员关系报告报文，因此当其对应的动态成员端口的老化定时器超时后，AP 就会将该端口对应的转发表项从转发表中删除。

运行 IGMPv2 或 IGMPv3 的主机离开组播组时，会通过发送 IGMP 离开组报文，以通知组播路由器自己离开了某个组播组。当 AP 从某动态成员端口上收到 IGMP 离开组报文时，首先判断要离开的组播组所对应的转发表项是否存在，以及该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：

- 如果不存在该组播组对应的转发表项，或者该组播组对应转发表项的出端口列表中不包含该端口，AP 不会向任何端口转发该报文，而将其直接丢弃；
- 如果存在该组播组对应的转发表项，且该组播组对应转发表项的出端口列表中包含该端口，AP 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组播组的其它成员，所以 AP 不会立刻把该端口从该组播组所对应转发表项的出端口列表中删除，而是重置其老化定时器。

当 IGMP 查询器收到 IGMP 离开组报文后，从中解析出主机要离开的组播组的地址，并通过接收端口向该组播组发送 IGMP 特定组查询报文。AP 在收到 IGMP 特定组查询报文后，将其通过 VLAN 内的所有路由器端口和该组播组的所有成员端口转发出去。对于 IGMP 离开组报文的接收端口（假定为动态成员端口），AP 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 IGMP 成员关系报告报文，则表示该端口下还有该组播组的成员，于是重置其老化定时器；
- 如果没有从该端口收到主机响应特定组查询的 IGMP 成员关系报告报文，则表示该端口下已没有该组播组的成员，则在其老化时间超时后，将其从该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 IGMP 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 IGMP Snooping配置任务简介

表1-2 IGMP Snooping 配置任务简介

配置任务		说明	详细配置
配置IGMP Snooping基本功能	使能IGMP Snooping	必选	1.3.2
	配置IGMP Snooping版本	可选	1.3.3
配置IGMP Snooping端口功能	配置动态端口老化定时器	可选	1.4.2
	配置静态端口	可选	1.4.3
	配置模拟主机加入	可选	1.4.4
	配置端口快速离开	可选	1.4.5
	禁止端口成为动态路由器端口	可选	1.4.6
配置IGMP Snooping查询器	使能IGMP Snooping查询器	可选	1.5.2
	配置IGMP查询和响应	可选	1.5.3
	配置IGMP查询报文源IP地址	可选	1.5.4
配置IGMP Snooping策略	配置组播组过滤器	可选	1.6.2
	配置丢弃未知组播数据报文	可选	1.6.3
	配置IGMP成员关系报告报文抑制	可选	1.6.4
	配置端口加入的组播组最大数量	可选	1.6.5
	配置组播组替换	可选	1.6.6
	配置IGMP报文的802.1p优先级	可选	1.6.7
	配置IGMP Snooping主机跟踪功能	可选	1.6.8
	配置PIM Hello报文代理功能	可选	1.6.9

说明

对于 IGMP Snooping 的相关配置来说:

- IGMP-Snooping 视图下的配置对所有 VLAN 都有效，VLAN 视图下的配置只对当前 VLAN 有效。对于某 VLAN 来说，优先采用该 VLAN 视图下的配置，只有当在该 VLAN 视图下没有进行配置时，才采用 IGMP-Snooping 视图下的相应配置。
- IGMP-Snooping 视图下的配置对所有端口都有效；二层以太网接口视图下的配置只对当前端口有效；端口组视图下的配置对当前端口组中的所有端口有效。对于某端口来说，优先采用二层以太网接口视图或端口组视图下的配置，只有当在上述视图下没有进行配置时，才采用 IGMP-Snooping 视图下的相应配置。

1.3 配置IGMP Snooping基本功能

1.3.1 配置准备

在配置 IGMP Snooping 基本功能之前，需完成以下任务：

- 配置相应 VLAN

在配置 IGMP Snooping 基本功能之前，需准备以下数据：

- IGMP Snooping 的版本

1.3.2 使能IGMP Snooping

表1-3 使能 IGMP Snooping

操作	命令	说明
进入系统视图	**system-view**	-
全局使能IGMP Snooping，并进入IGMP-Snooping视图	**igmp-snooping**	必选 缺省情况下，IGMP Snooping处于关闭状态
退回系统视图	**quit**	-
进入VLAN视图	**vlan** *vlan-id*	-
在VLAN内使能IGMP Snooping	**igmp-snooping enable**	必选 缺省情况下，VLAN内的IGMP Snooping处于关闭状态

说明

- 在 VLAN 内使能 IGMP Snooping 之前，必须先在系统视图下全局使能 IGMP Snooping，否则将无法在 VLAN 内使能 IGMP Snooping。
- 在指定 VLAN 内使能了 IGMP Snooping 之后，IGMP Snooping 功能只在属于该 VLAN 的端口上生效。

1.3.3 配置IGMP Snooping版本

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

- 当 IGMP Snooping 的版本为 2 时，IGMP Snooping 能够对 IGMPv1 和 IGMPv2 的报文进行处理，对 IGMPv3 的报文则不进行处理，而是在 VLAN 内将其广播；
- 当 IGMP Snooping 的版本为 3 时，IGMP Snooping 能够对 IGMPv1、IGMPv2 和 IGMPv3 的报文进行处理。

表1-4 配置 IGMP Snooping 版本

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入VLAN视图	**vlan** *vlan-id*	-
配置IGMP Snooping的版本	**igmp-snooping version** *version-number*	必选 缺省情况下，IGMP Snooping的版本为2

注意

当 IGMP Snooping 的版本由版本 3 切换到版本 2 时，系统将清除所有通过动态加入的 IGMP Snooping 转发表项；对于在版本 3 下通过手工配置而静态加入的 IGMP 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组播组，而没有指定组播源，则这些转发表项将不会被清除；
- 如果配置的是指定了组播源的静态加入组播源组，则这些转发表项将会被清除，并且当再次切换回版本 3 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”。

1.4 配置IGMP Snooping端口功能

1.4.1 配置准备

在配置 IGMP Snooping 端口功能之前，需完成以下任务：

- 在 VLAN 内使能 IGMP Snooping
- 配置相应端口组

在配置 IGMP 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
- 组播组和组播源的地址

1.4.2 配置动态端口老化定时器

对于动态路由器端口，如果在其老化时间超时前没有收到 IGMP 普遍组查询报文或者 PIM Hello 报文，AP 将把该端口从路由器端口列表中删除。

对于动态成员端口，如果在其老化时间超时前没有收到该组播组的 IGMP 成员关系报告报文，AP 将把该端口从该组播组所对应转发表项的出端口列表中删除。

如果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。

1. 全局配置动态端口老化定时器

表1-5 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	**system-view**	-

操作	命令	说明
进入IGMP-Snooping视图	**igmp-snooping**	-
配置动态路由器端口老化时间	**router-aging-time** *interval*	必选 缺省情况下，动态路由器端口的老化时间为105秒
配置动态成员端口老化时间	**host-aging-time** *interval*	必选 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1-6 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	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
配置动态路由器端口老化时间	**igmp-snooping router-aging-time** *interval*	必选 缺省情况下，动态路由器端口的老化时间为105秒
配置动态成员端口老化时间	**igmp-snooping host-aging-time** *interval*	必选 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组播组或组播源组的组播数据，可以配置该端口静态加入该组播组或组播源组，成为静态成员端口。

表1-7 配置静态端口

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置静态成员端口		**igmp-snooping static-group** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*	必选 缺省情况下，端口不是静态成员端口

说明

- 静态成员端口不会对 IGMP 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 IGMP 成员关系报告报文或 IGMP 离开组报文。
- 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

通常情况下，运行 IGMP 的主机会对 IGMP 查询器发出的查询报文进行响应。如果主机由于某种原因无法响应，就可能导致组播路由器认为该网段没有该组播组的成员，从而取消相应的转发路径。为避免这种情况的发生，可以将 AP 的端口配置成为组播组成员（即配置模拟主机加入）。当收到 IGMP 查询报文时由模拟主机进行响应，从而保证该 AP 能够继续收到组播报文。

模拟主机加入功能的实现原理如下：

- 在某端口上使能模拟主机加入功能时，AP 会通过该端口主动发送一个 IGMP 成员关系报告报文；
- 在某端口上使能了模拟主机加入功能后，当收到 IGMP 普遍组查询报文时，AP 会通过该端口响应一个 IGMP 成员关系报告报文；
- 在某端口上关闭模拟主机加入功能时，AP 会通过该端口发送一个 IGMP 离开组报文。

表1-8 配置模拟主机加入

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置模拟主机加入组播组或组播源组		**igmp-snooping host-join** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*	必选 缺省情况下，没有配置模拟主机加入组播组或组播源组

说明

- 每配置一次模拟主机加入，即相当于启动了一台独立的主机。例如，当收到 IGMP 查询报文时，每条配置所对应的模拟主机将分别进行响应。
- 与静态成员端口不同，配置了模拟主机加入的端口会作为动态成员端口而参与动态成员端口的老化过程。

1.4.5 配置端口快速离开

端口快速离开是指当 AP 从某端口收到主机发送的离开某组播组的 IGMP 离开组报文时，直接把该端口从对应转发表项的出端口列表中删除。此后，当 AP 收到对该组播组的 IGMP 特定组查询报文时，AP 将不再向该端口转发。

在 AP 上，在只连接有一个接收者的端口上，可以通过使能端口快速离开功能来节约带宽和资源；而在连接有多个接收者的端口上，如果 AP 或该端口所在的 VLAN 已使能了丢弃未知组播数据报文功能，则不要再使能端口快速离开功能，否则，一个接收者的离开将导致该端口下属于同一组播组的其它接收者无法收到组播数据。

1. 全局配置端口快速离开

表1-9 全局配置端口快速离开

操作	命令	说明
进入系统视图	**system-view**	-
进入IGMP-Snooping视图	**igmp-snooping**	-
使能端口快速离开功能	**fast-leave** [**vlan** *vlan-list*]	必选 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1-10 在端口上配置端口快速离开

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
使能端口快速离开功能		**igmp-snooping fast-leave** [**vlan** *vlan-list*]	必选 缺省情况下，端口快速离开功能处于关闭状态

1.4.6 禁止端口成为动态路由器端口

目前，在组播用户接入网络中存在以下问题：

- 如果 AP 收到了某用户主机发来的 IGMP 普遍组查询报文或 PIM Hello 报文，那么该主机所在的端口就将成为动态路由器端口，从而使 VLAN 内的所有组播报文都会向该端口转发，导致该用户主机收到的组播报文失控。
- 同时，用户主机发送 IGMP 普遍组查询报文或 PIM Hello 报文，也会影响该接入网络中三层设备上的组播路由协议状态（如影响 IGMP 查询器或 DR 的选举），严重时可能导致网络中断。

当禁止某端口成为动态路由器端口后，即使该端口收到了 IGMP 普遍组查询报文或 PIM Hello 报文，该端口也不会成为动态路由器端口，从而能够有效解决上述问题，提高网络的安全性和对组播用户的控制能力。

表1-11 禁止端口成为动态路由器端口

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
禁止端口成为动态路由器端口		**igmp-snooping router-port-deny** [**vlan** *vlan-list*]	必选 缺省情况下，不禁止端口成为动态路由器端口


说明

本配置与静态路由器端口的配置互不影响。

1.5 配置IGMP Snooping查询器

1.5.1 配置准备

在配置 IGMP Snooping 查询器之前，需完成以下任务：

- 在 VLAN 内使能 IGMP Snooping

在配置 IGMP Snooping 查询器之前，需准备以下数据：

- 发送 IGMP 普遍组查询报文的时间间隔
- 发送 IGMP 特定组查询报文的时间间隔
- IGMP 普遍组查询的最大响应时间
- IGMP 普遍组查询报文的源 IP 地址
- IGMP 特定组查询报文的源 IP 地址

1.5.2 使能IGMP Snooping查询器

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

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 IGMP，因此无法实现 IGMP 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 IGMP Snooping 查询器，使二层设备能够在数据链路层建立并维护组播转发表项，从而在数据链路层正常转发组播数据。

1. 在VLAN内使能IGMP Snooping查询器

表1-12 在 VLAN 内使能 IGMP Snooping 查询器

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
使能IGMP Snooping查询器	**igmp-snooping querier**	必选 缺省情况下，IGMP Snooping查询器处于关闭状态

注意

尽管 IGMP Snooping 查询器并不参与 IGMP 查询器的选举，但在运行了 IGMP 的组播网络中，配置 IGMP Snooping 查询器不但没有实际的意义，反而可能会由于其发送的 IGMP 普遍组查询报文的源 IP 地址较小而影响 IGMP 查询器的选举。

1.5.3 配置IGMP查询和响应

可以根据网络的实际情况来修改发送 IGMP 普遍组查询报文的时间间隔。

在收到 IGMP 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 IGMP 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组播组发送 IGMP 成员关系报告报文。

合理配置 IGMP 查询的最大响应时间，既可以使主机对 IGMP 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 IGMP 普遍组查询报文来说，通过配置 IGMP 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 IGMP 特定组查询报文来说，所配置的发送 IGMP 特定组查询报文的时间间隔将被填充到其最大响应时间字段。也就是说，IGMP 特定组查询的最大响应时间从数值上与发送 IGMP 特定组查询报文的时间间隔相同。

1. 全局配置IGMP查询和响应

表1-13 全局配置 IGMP 查询和响应

操作	命令	说明
进入系统视图	**system-view**	-
进入IGMP-Snooping视图	**igmp-snooping**	-
配置IGMP普遍组查询的最大响应时间	**max-response-time** *interval*	必选 缺省情况下，IGMP普遍组查询的最大响应时间为10秒

操作	命令	说明
配置发送IGMP特定组查询报文的时间间隔	**last-member-query-interval** *interval*	必选 缺省情况下，发送IGMP特定组查询报文的时间间隔为1秒

2. 在VLAN内配置IGMP查询和响应

表1-14 在 VLAN 内配置 IGMP 查询和响应

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
配置发送IGMP普遍组查询报文的时间间隔	**igmp-snooping query-interval** *interval*	必选 缺省情况下，发送IGMP普遍组查询报文的时间间隔为60秒
配置IGMP普遍组查询的最大响应时间	**igmp-snooping max-response-time** *interval*	必选 缺省情况下，IGMP普遍组查询的最大响应时间为10秒
配置发送IGMP特定组查询报文的时间间隔	**igmp-snooping last-member-query-interval** *interval*	必选 缺省情况下，发送IGMP特定组查询报文的时间间隔为1秒

注意

应确保发送 IGMP 普遍组查询报文的时间间隔大于 IGMP 普遍组查询的最大响应时间，否则有可能造成对组播组成员的误删。

1.5.4 配置IGMP查询报文源IP地址

对于收到源 IP 地址为 0.0.0.0 的查询报文的端口，AP 不会将其设置为动态路由器端口，从而影响数据链路层组播转发表项的建立，最终导致组播数据无法正常转发。

当由二层设备充当 IGMP Snooping 查询器时，可以把 IGMP 查询报文的源 IP 地址配置为一个有效的 IP 地址以避免上述问题的出现。

1. 在VLAN内配置IGMP查询报文源IP地址

表1-15 在 VLAN 内配置 IGMP 查询报文源 IP 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-

操作	命令	说明
配置IGMP普遍组查询报文源IP地址	**igmp-snooping general-query source-ip** { *ip-address* | **current-interface** }	必选 缺省情况下，IGMP普遍组查询报文的源IP地址为0.0.0.0
配置IGMP特定组查询报文源IP地址	**igmp-snooping special-query source-ip** { *ip-address* | **current-interface** }	必选 缺省情况下，IGMP特定组查询报文的源IP地址为0.0.0.0

注意

IGMP 查询报文源 IP 地址的改变可能会影响网段内 IGMP 查询器的选举。

1.6 配置IGMP Snooping策略

1.6.1 配置准备

在配置 IGMP Snooping 策略之前，需完成以下任务：

- 在 VLAN 内使能 IGMP Snooping

在配置 IGMP Snooping 策略之前，需准备以下数据：

- 组播组过滤的 ACL 规则
- 端口加入的组播组最大数量
- IGMP 报文的 802.1p 优先级

1.6.2 配置组播组过滤器

在使能了 IGMP Snooping 的 AP 上，通过配置组播组过滤器，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 IGMP 成员关系报告报文，该报文到达 AP 后，进行 ACL 检查：如果该接收端口可以加入这个组播组，则将其列入到 IGMP Snooping 转发表中；否则 AP 就丢弃该报文。这样，未通过 ACL 检查的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。

1. 全局配置组播组过滤器

表1-16 全局配置组播组过滤器

操作	命令	说明
进入系统视图	**system-view**	-
进入IGMP-Snooping视图	**igmp-snooping**	-
配置组播组过滤器	**group-policy** *acl-number* [**vlan** *vlan-list*]	必选 缺省情况下，没有配置全局组播组过滤器，即各VLAN内主机可以加入任意合法的组播组

2. 在端口上配置组播组过滤器

表1-17 在端口上配置组播组过滤器

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置组播组过滤器		**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	必选 缺省情况下，端口上没有配置组播组过滤器，即该端口下的主机可以加入任意合法的组播组

1.6.3 配置丢弃未知组播数据报文

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

- 当使能了丢弃未知组播数据报文功能时，AP 将丢弃所有收到的未知组播数据报文；
- 当关闭了丢弃未知组播数据报文功能时，AP 将在未知组播数据报文所属的 VLAN 内广播该报文。

1. 全局配置丢弃未知组播数据报文

表1-18 全局配置丢弃未知组播数据报文

操作	命令	说明
进入系统视图	**system-view**	-
进入IGMP-Snooping视图	**igmp-snooping**	-
使能丢弃未知组播数据报文功能	**drop-unknown**	必选 缺省情况下，丢弃未知组播数据报文的功能处于关闭状态，即对未知组播数据报文进行广播

2. 在VLAN内配置丢弃未知组播数据报文

表1-19 在 VLAN 内配置丢弃未知组播数据报文

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
使能丢弃未知组播数据报文功能	**igmp-snooping drop-unknown**	必选 缺省情况下，丢弃未知组播数据报文的功能处于关闭状态，即对未知组播数据报文进行广播

说明

对于同时支持 **drop-unknown** 和 **igmp-snooping drop-unknown** 这两条命令的设备来说，IGMP-Snooping 视图和 VLAN 视图下的配置是互斥的。也就是说，当在 IGMP-Snooping 视图下全局使能了丢弃未知组播数据报文的功能后，不允许在 VLAN 视图下使能或关闭该功能，反之亦然。

1.6.4 配置IGMP成员关系报告报文抑制

当二层设备收到来自某组播组成员的 IGMP 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 IGMP 成员关系报告报文。

当使能了 IGMP 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组播组内的第一个 IGMP 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组播组的其它 IGMP 成员关系报告报文，这样可以减少网络中的报文数量。

表1-20 配置 IGMP 成员关系报告报文抑制

操作	命令	说明
进入系统视图	**system-view**	-
进入IGMP-Snooping视图	**igmp-snooping**	-
使能IGMP成员关系报告报文抑制功能	**report-aggregation**	必选 缺省情况下，IGMP成员关系报告报文抑制功能处于使能状态

1.6.5 配置端口加入的组播组最大数量

通过配置端口加入的组播组最大数量，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1-21 配置端口加入的组播组最大数量

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口加入的组播组最大数量		**igmp-snooping group-limit** *limit* [**vlan** *vlan-list*]	必选 缺省情况下，端口加入的组播组最大数量与设备的型号有关，请以设备的实际情况为准

说明

在配置端口加入的组播组最大数量时，如果当前端口上的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 IGMP Snooping 转发表中删除，该端口下的主机都需要重新加入组播组，直至该端口上的组播组数量达到限制值为止。其中，如果该端口已配置为静态成员端口，系统会将静态成员端口的配置重新生效一次；如果在该端口上配置了模拟主机加入，系统在收到模拟主机发来的报告报文之后才会重新建立相应的转发表项。

1.6.6 配置组播组替换

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

针对以上情况，可以在 AP 或者某些端口上使能组播组替换功能。当 AP 或端口上加入的组播组数量已达到限定值时：

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

1. 全局配置组播组替换

表1-22 全局配置组播组替换

操作	命令	说明
进入系统视图	**system-view**	-
进入IGMP-Snooping视图	**igmp-snooping**	-
使能组播组替换功能	**overflow-replace** [**vlan** *vlan-list*]	必选 缺省情况下，组播组替换功能处于关闭状态

2. 在端口上配置组播组替换

表1-23 在端口上配置组播组替换

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
使能组播组替换功能		**igmp-snooping overflow-replace** [**vlan** *vlan-list*]	必选 缺省情况下，组播组替换功能处于关闭状态

注意

当端口加入的组播组最大数量取缺省值时，组播组替换功能将不会生效，因此在使能组播组替换功能之前，必须先将端口通过的组播组最大数量配置为非缺省值（具体配置过程请参见“1.6.5 配置端口加入的组播组最大数量”）。

1.6.7 配置IGMP报文的 802.1p优先级

可以通过本配置来改变 IGMP 报文的 802.1p 优先级。当 AP 的出端口发生拥塞时，AP 通过识别报文的 802.1p 优先级，优先发送优先级较高的报文。

1. 全局配置IGMP报文的 802.1p优先级

表1-24 全局配置 IGMP 报文的 802.1p 优先级

操作	命令	说明
进入系统视图	**system-view**	-
进入IGMP-Snooping视图	**igmp-snooping**	-
配置IGMP报文的802.1p优先级	**dot1p-priority** *priority-number*	必选 缺省情况下，IGMP报文的802.1p优先级为0

说明

本全局配置对所有 VLAN 都有效。

2. 在VLAN内配置IGMP报文的 802.1p优先级

表1-25 在 VLAN 内配置 IGMP 报文的 802.1p 优先级

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
配置IGMP报文的802.1p优先级	**igmp-snooping dot1p-priority** *priority-number*	必选 缺省情况下，IGMP报文的802.1p优先级为0

1.6.8 配置IGMP Snooping主机跟踪功能

通过使能 IGMP Snooping 主机跟踪功能，可以使 AP 能够记录正在接收组播数据的成员主机信息（包括主机的 IP 地址、运行时间和超时时间等），以便于网络管理员对这些主机进行监控和管理。

1. 全局配置IGMP Snooping主机跟踪功能

表1-26 全局配置 IGMP Snooping 主机跟踪功能

操作	命令	说明
进入系统视图	**system-view**	-
进入IGMP-Snooping视图	**igmp-snooping**	-
全局使能IGMP Snooping主机跟踪功能	**host-tracking**	必选 缺省情况下，IGMP Snooping主机跟踪功能处于关闭状态

2. 在VLAN内配置IGMP Snooping主机跟踪功能

表1-27 在 VLAN 内配置 IGMP Snooping 主机跟踪功能

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
在VLAN内使能IGMP Snooping主机跟踪功能	**igmp-snooping host-tracking**	必选 缺省情况下，IGMP Snooping主机跟踪功能处于关闭状态

1.6.9 配置PIM Hello报文代理功能

在地铁运行环境的 WLAN 网络中，为了实现 Mesh 链路切换之后，车载 AP 能够快速将组播流量从新的链路引下来，需要在车载 AP 检测到 Mesh 链路切换之后，将之前记录的 PIM Hello 报文从新的 Mesh 链路发送出去，让上游设备能够快速维护路由端口，从而保证组播流量能够从此路由端口快速转发下来。

表1-28 配置 PIM Hello 报文代理功能

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
开启PIM Hello报文代理功能	**igmp-snooping** **pim-hello-proxy enable**	必选 缺省情况下，PIM Hello报文代理功能处于关闭状态

1.7 IGMP 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 IGMP 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** 命令可以清除组播组信息。

表1-29 IGMP Snooping 显示和维护

操作	命令
查看IGMP Snooping组的信息	**display igmp-snooping group** [**vlan** *vlan-id*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看IGMP Snooping跟踪的主机信息	**display igmp-snooping host vlan** *vlan-id* **group** *group-address* [**source** *source-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看IGMP Snooping监听到的IGMP报文的统计信息	**display igmp-snooping statistics** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除IGMP Snooping组的动态加入记录	**reset igmp-snooping group** { *group-address* | **all** } [**vlan** *vlan-id*]
清除IGMP Snooping监听到的所有IGMP报文的统计信息	**reset igmp-snooping statistics**

1.8 IGMP Snooping典型配置举例

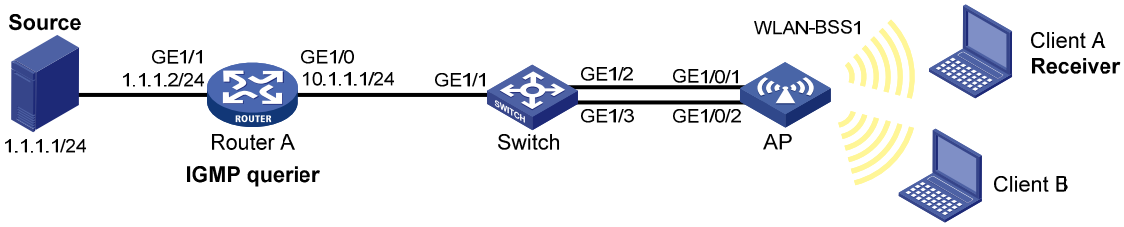
1.8.1 组策略配置举例

1. 组网需求

- 如 图 1-3 所示，Router A通过GigabitEthernet 1/1 接口连接组播源（Source），通过GigabitEthernet 1/0 接口连接Switch，Switch和AP之间配置链路聚合；
- Router A 上运行 IGMPv2，Switch 和 AP 上运行版本 2 的 IGMP Snooping，并由 Router A 充当 IGMP 查询器；
- 在无线客户 Client A 上，通过组播客户端软件（比如 VLC media player）加入组播组 224.1.1.1，使连接在 AP 上的接收者（Receiver）Client A 只能接收发往组播组 224.1.1.1 的组播数据；

2. 组网图

图1-3 组策略配置组网图



3. 配置步骤

(1) 配置 IP 地址

请按照 图 1-3 配置各接口的IP地址和子网掩码，具体配置过程略。

(2) 配置 RouterA

使能 IP 组播路由，在各接口上使能 PIM-DM，并在接口 GigabitEthernet 1/0 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing-enable
```

```
[RouterA] interface GigabitEthernet 1/0
[RouterA-GigabitEthernet1/0] igmp enable
[RouterA-GigabitEthernet1/0] pim dm
[RouterA-GigabitEthernet1/0] quit
[RouterA] interface GigabitEthernet 1/1
[RouterA-GigabitEthernet1/1] pim dm
[RouterA-GigabitEthernet1/1] quit
```

(3) 配置 Switch

全局使能 IGMP Snooping。

```
<Switch> system-view
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
```

创建 VLAN 100，把端口 GigabitEthernet 1/1 到 GigabitEthernet 1/3 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping。

```
[Switch] vlan 100
[Switch-vlan100] port GigabitEthernet 1/1 to GigabitEthernet 1/3
[Switch-vlan100] igmp-snooping enable
[Switch-vlan100] quit
```

创建二层聚合端口 1。

```
[Switch] interface Bridge-Aggregation 1
[Switch-Bridge-Aggregation1] quit
```

分别将端口 GigabitEthernet 1/2 至 GigabitEthernet 1/3 加入到聚合组 1 中。

```
[Switch] interface GigabitEthernet 1/2
[Switch-GigabitEthernet1/2] port link-aggregation group 1
[Switch-GigabitEthernet1/2] quit
[Switch] interface GigabitEthernet 1/3
[Switch-GigabitEthernet1/3] port link-aggregation group 1
[Switch-GigabitEthernet1/3] quit
```

配置二层聚合接口 1 为 Trunk 端口，并允许 VLAN 100 的报文通过。

```
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] port link-type trunk
[Switch-Bridge-Aggregation1] port trunk permit vlan 100
```

将二层聚合口配置为 IGMP Snooping 静态路由端口。

```
[Switch-Bridge-Aggregation1] igmp-snooping static-router-port vlan 100
[Switch-Bridge-Aggregation1] quit
```

(4) 配置 AP

全局使能 IGMP Snooping。

```
<AP> system-view
[AP] igmp-snooping
[AP-igmp-snooping] quit
```

创建 VLAN 100，把端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 WLAN-BSS1 添加到该 VLAN 中；在该 VLAN 内使能 IGMP Snooping，并使能丢弃未知组播数据报文功能。

```
[AP] vlan 100
[AP-vlan100] port GigabitEthernet 1/0/1
[AP-vlan100] port WLAN-BSS1
```

```
[AP-vlan100] port GigabitEthernet 1/0/2
[AP-vlan100] port WLAN-BSS1
[AP-vlan100] igmp-snooping enable
[AP-vlan100] igmp-snooping drop-unknown
[AP-vlan100] quit
```

创建二层聚合端口 1。

```
[AP] interface Bridge-Aggregation 1
[AP-Bridge-Aggregation1] quit
```

分别将端口 GigabitEthernet 1/0/1 至 GigabitEthernet 1/0/2 加入到聚合组 1 中。

```
[AP] interface GigabitEthernet 1/0/1
[AP-GigabitEthernet1/0/1] port link-aggregation group 1
[AP-GigabitEthernet1/0/1] quit
[AP] interface GigabitEthernet 1/0/2
[AP-GigabitEthernet1/0/2] port link-aggregation group 1
[AP-GigabitEthernet1/0/2] quit
```

配置二层聚合接口 1 为 Trunk 端口，并允许 VLAN 100 的报文通过。

```
[AP] interface bridge-aggregation 1
[AP-Bridge-Aggregation1] port link-type trunk
[AP-Bridge-Aggregation1] port trunk permit vlan 100
```

配置组播组过滤器，使 VLAN 100 内的主机只能加入组播组 224.1.1.1。

```
[AP] acl number 2001
[AP-acl-basic-2001] rule permit source 224.1.1.1 0
[AP-acl-basic-2001] quit
[AP] igmp-snooping
[AP-igmp-snooping] group-policy 2001 vlan 100
[AP-igmp-snooping] quit
```

4. 检验配置效果

在 Client A 上开启组播软件，加入所配置的组播组，查看 AP 上 VLAN 100 内 IGMP Snooping 组播组的详细信息。

```
[AP] display igmp-snooping group vlan 100 verbose
    Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Port flags: D-Dynamic port, S-Static port, C-Copy port
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 1 port(s).
           BAGG1              (D) ( 00:01:31 )
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Attribute:    Host Port
          Host port(s):total 2 port(s).
            WLAN-BSS1            (D) ( 00:04:07 )
```

```
MAC group(s):
  MAC group address:0100-5e01-0101
      Host port(s):total 2 port(s).
        WLAN-BSS1
```

由此可见，AP 上的端口 WLAN-BSS1 已经加入了组播组 224.1.1.1，VLAN 100 内没有其它组播组，并且 Client A 可以接收组播组 224.1.1.1 的组播数据。

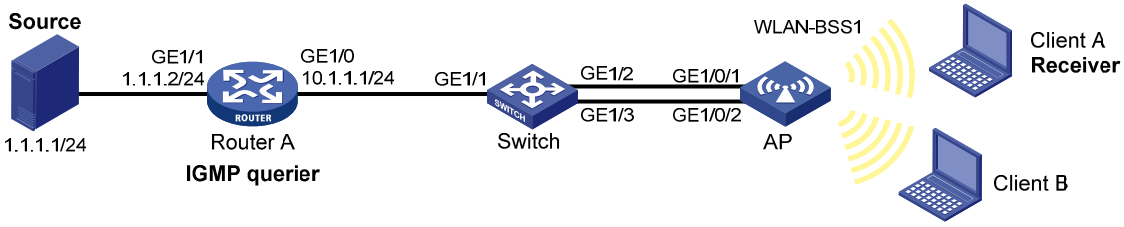
1.8.2 静态成员端口配置举例

1. 组网需求

- 如 图 1-4 所示，Router A通过GigabitEthernet 1/1 接口连接组播源（Source），通过 GigabitEthernet 1/0 接口连接Switch，Switch和AP之间配置链路聚合；
- Router A 上运行 IGMPv2，Switch 和 AP 上运行版本 2 的 IGMP Snooping，并由 Router A 充当 IGMP 查询器；
- 通过在 AP 上配置静态成员端口，使无线客户端 Client 上不需要通过组播客户端软件加入组播组 224.1.1.1 即可接收组播数据。

2. 组网图

图1-4 静态端口配置组网图



3. 配置步骤

(1) 配置 IP 地址

请按照 图 1-3 配置各接口的IP地址和子网掩码，具体配置过程略。

(2) 配置 RouterA

使能 IP 组播路由，在各接口上使能 PIM-DM，并在接口 GigabitEthernet 1/0 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface GigabitEthernet 1/0
[RouterA-GigabitEthernet1/0] igmp enable
[RouterA-GigabitEthernet1/0] pim dm
[RouterA-GigabitEthernet1/0] quit
[RouterA] interface GigabitEthernet 1/1
[RouterA-GigabitEthernet1/1] pim dm
[RouterA-GigabitEthernet1/1] quit
```

(3) 配置 Switch

全局使能 IGMP Snooping。

```
<Switch> system-view
```

```
[Switch] igmp-snooping
[Switch-igmp-snooping] quit
```
创建 VLAN 100，把端口 GigabitEthernet 1/1 到 GigabitEthernet 1/3 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping。
```
[Switch] vlan 100
[Switch-vlan100] port GigabitEthernet 1/1 to GigabitEthernet 1/3
[Switch-vlan100] igmp-snooping enable
[Switch-vlan100] quit
```
创建二层聚合端口 1。
```
[Switch] interface Bridge-Aggregation 1
[Switch-Bridge-Aggregation1] quit
```
分别将端口 GigabitEthernet 1/2 至 GigabitEthernet 1/3 加入到聚合组 1 中。
```
[Switch] interface GigabitEthernet 1/2
[Switch-GigabitEthernet1/2] port link-aggregation group 1
[Switch-GigabitEthernet1/2] quit
[Switch] interface GigabitEthernet 1/3
[Switch-GigabitEthernet1/3] port link-aggregation group 1
[Switch-GigabitEthernet1/3] quit
```
配置二层聚合接口 1 为 Trunk 端口，并允许 VLAN 100 的报文通过。
```
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] port link-type trunk
[Switch-Bridge-Aggregation1] port trunk permit vlan 100
```
将二层聚合口配置为 IGMP Snooping 静态路由端口。
```
[Switch-Bridge-Aggregation1] igmp-snooping static-router-port vlan 100
[Switch-Bridge-Aggregation1] quit
```
(4) 配置 AP

全局使能 IGMP Snooping。
```
<AP> system-view
[AP] igmp-snooping
[AP-igmp-snooping] quit
```
创建 VLAN 100，把端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、WLAN-BSS1 添加到该 VLAN 中；在该 VLAN 内使能 IGMP Snooping，并使能丢弃未知组播数据报文功能。
```
[AP] vlan 100
[AP-vlan100] port GigabitEthernet 1/0/1
[AP-vlan100] port GigabitEthernet 1/0/2
[AP-vlan100] port WLAN-BSS1
[AP-vlan100] igmp-snooping enable
[AP-vlan100] igmp-snooping drop-unknown
[AP-vlan100] quit
```
创建二层聚合端口 1。
```
[AP] interface Bridge-Aggregation 1
[AP-Bridge-Aggregation1] quit
```
分别将端口 GigabitEthernet 1/0/1 至 GigabitEthernet 1/0/2 加入到聚合组 1 中。
```
[AP] interface GigabitEthernet 1/0/1
[AP-GigabitEthernet1/0/1] port link-aggregation group 1
```

```
[AP-GigabitEthernet1/0/1] quit
[AP] interface GigabitEthernet 1/0/2
[AP-GigabitEthernet1/0/2] port link-aggregation group 1
[AP-GigabitEthernet1/0/2] quit
```

配置二层聚合接口 1 为 Trunk 端口，并允许 VLAN 100 的报文通过。

```
[AP] interface bridge-aggregation 1
[AP-Bridge-Aggregation1] port link-type trunk
[AP-Bridge-Aggregation1] port trunk permit vlan 100
```

将二层聚合口配置为 IGMP Snooping 静态成员端口。

```
[AP-Bridge-Aggregation1] igmp-snooping static-group 224.1.1.1 vlan 100
[AP-Bridge-Aggregation1] quit
```

(5) 检验配置效果

查看 AP 上 VLAN 100 内 IGMP Snooping 组的详细信息。

```
[AP] display igmp-snooping group vlan 100 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Attribute:    Host Port
          Host port(s):total 1 port(s).
            BAGG1                (S)
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 1 port(s).
            BAGG1                (S)
```

由此可见，AP 上的二层聚合端口 BAGG1 已经成为了组播组 224.1.1.1 的静态成员端口，VLAN 100 内没有其它组播组，并且 Client A 可以接收组播组 224.1.1.1 的组播数据。。

1.9 常见配置错误举例

1.9.1 AP不能实现二层组播

1. 故障现象

AP 不能实现 IGMP Snooping 二层组播功能。

2. 分析

- IGMP Snooping 没有使能；
- 设备与主机上的 IGMP Snooping 版本不一致。

3. 处理过程

(1) 使用 **display current-configuration** 命令查看 IGMP Snooping 的运行状态。

(2) 如果是没有使能 IGMP Snooping，则需先在系统视图下使用 **igmp-snooping** 命令全局使能 IGMP Snooping，然后在 VLAN 视图下使用 **igmp-snooping enable** 命令使能 VLAN 内的 IGMP Snooping。

(3) 如果只是没有在相应 VLAN 下使能 IGMP Snooping，则只需在 VLAN 视图下使用 **igmp-snooping enable** 命令使能 VLAN 内的 IGMP Snooping。

(4) 如果 IGMP Snooping 使能了，但组播功能仍然不可用，可能是主机上使用的 IGMP Snooping 的版本为 3，但设备上默认的 IGMP Snooping 版本是 2，从而导致设备上组播表项建立失败，此时可以使用命令 **igmp-snooping version 3** 把设备的 IGMP Snooping 版本配置为 3。

1.9.2 配置的组播组策略不生效

1. 故障现象

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

2. 分析

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

3. 处理过程

(1) 使用 **display acl** 命令查看所配置的 ACL 规则，检查其是否与所要实现的组播组过滤策略相符合。

(2) 在 IGMP-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组播组策略。如果没有，则使用 **group-policy** 或 **igmp-snooping group-policy** 命令应用正确的组播组策略。

(3) 使用 **display current-configuration** 命令查看是否已使能丢弃未知组播数据报文的功能。如果没有使能，则使用 **drop-unknown** 或 **igmp-snooping drop-unknown** 命令使能丢弃未知组播数据报文功能。

目 录

1 MLD Snooping

说明

本章所指的路由器代表了一般意义下的路由设备，以及配置了路由功能的无线接入点设备。为提高可读性，在手册的描述中将不另行说明。

1.1 MLD Snooping简介

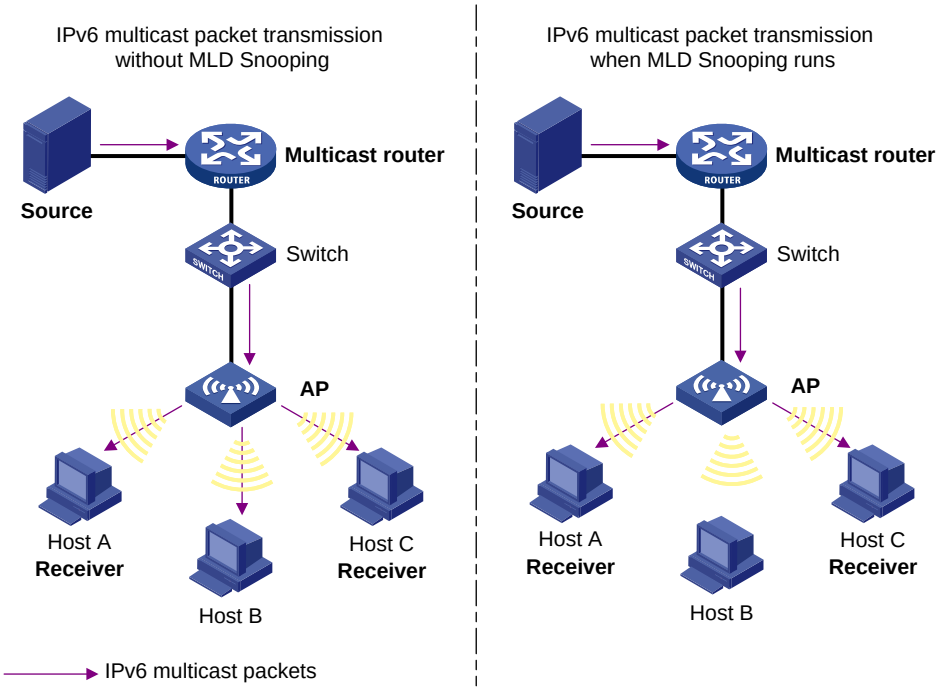
MLD Snooping 是 Multicast Listener Discovery Snooping（组播侦听者发现协议窥探）的简称。它是运行在二层设备上的 IPv6 组播约束机制，用于管理和控制 IPv6 组播组。

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（包括VLAN）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：

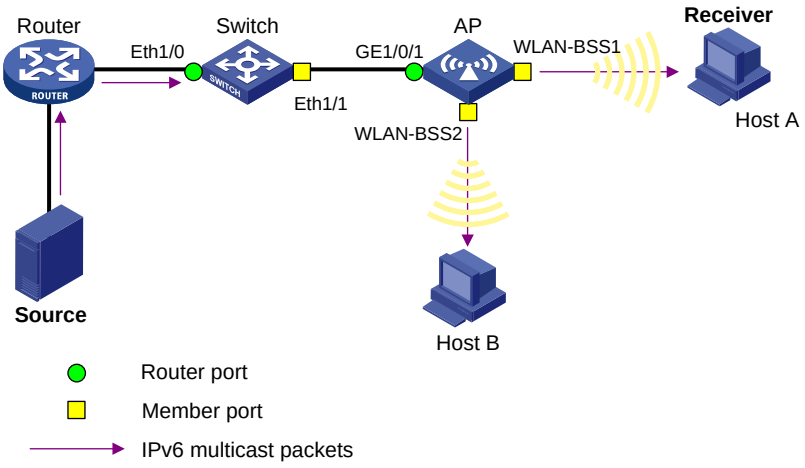
- 减少了二层网络中的广播报文，节约了网络带宽；
- 增强了 IPv6 组播信息的安全性；
- 为实现对每台主机的单独计费带来了方便。

1.1.2 MLD Snooping基本概念

1. MLD Snooping相关端口

如 图 1-2 所示，Router A连接组播源，在Switch和AP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）：交换机或 AP 上朝向三层组播设备（DR 或 MLD 查询器）一侧的端口，如 Switch 的 Ethernet1/0 端口和 AP 的 GigabitEthernet1/0/1 端口。交换机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，表示交换机上朝向 IPv6 组播组成员一侧的端口，如 Switch 的 Ethernet1/1 端口，以及 AP 的 WLAN-BSS1 和 WLAN-BSS2 端口。交换机或 AP 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交换机或 AP 上朝向组播路由器的端口，而不是指路由器上的端口。
- 如不特别指明，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 的交换机上或 AP，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。

---

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 AP 的动作
动态路由器端口老化定时器	AP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，AP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 AP 对不同 MLD 动作的具体处理方式如下：

注意

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，AP 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，AP 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。

说明

AP 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 AP 无法获知这些端口下还有该 IPv6 组播组的成员主机。

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，以通知组播路由器自己离开了某个 IPv6 组播组。当 AP 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，AP 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，AP 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 AP 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，而是重置其老化定时器。

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。AP 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），AP 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，则在其老化时间超时后，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	1.3.2

配置任务		说明	详细配置
	配置MLD Snooping版本	可选	1.3.3
配置MLD Snooping端口功能	配置动态端口老化定时器	可选	1.4.2
	配置静态端口	可选	1.4.3
	配置模拟主机加入	可选	1.4.4
	配置端口快速离开	可选	1.4.5
	禁止端口成为动态路由器端口	可选	1.4.6
配置MLD Snooping查询器	使能MLD Snooping查询器	可选	1.5.2
	配置MLD查询和响应	可选	1.5.3
	配置MLD查询报文源IPv6地址	可选	1.5.4
配置MLD Snooping策略	配置IPv6组播组过滤器	可选	1.6.2
	配置丢弃未知IPv6组播数据报文	可选	1.6.3
	配置MLD成员关系报告报文抑制	可选	1.6.4
	配置端口加入的IPv6组播组最大数量	可选	1.6.5
	配置IPv6组播组替换	可选	1.6.6
	配置MLD报文的802.1p优先级	可选	1.6.7
	配置MLD Snooping主机跟踪功能	可选	1.6.8

说明

对于 MLD Snooping 的相关配置来说:

- MLD-Snooping 视图下的配置对所有 VLAN 都有效，VLAN 视图下的配置只对当前 VLAN 有效。对于某 VLAN 来说，优先采用该 VLAN 视图下的配置，只有当在该 VLAN 视图下没有进行配置时，才采用 MLD-Snooping 视图下的相应配置。
- MLD-Snooping 视图下的配置对所有端口都有效；二层以太网接口视图下的配置只对当前端口有效；二层聚合接口视图下的配置只对当前接口有效；端口组视图下的配置对当前端口组中的所有端口有效。对于某端口来说，优先采用二层以太网接口视图、二层聚合接口视图或端口组视图下的配置，只有当在上述视图下没有进行配置时，才采用 MLD-Snooping 视图下的相应配置。
- 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：

- 使能 IPv6 转发功能
- 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

1.3.2 使能MLD Snooping

表1-3 使能 MLD Snooping

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

说明

- 在 VLAN 内使能 MLD Snooping 之前，必须先在系统视图下全局使能 MLD Snooping，否则将无法在 VLAN 内使能 MLD Snooping。
- 在指定 VLAN 内使能了 MLD Snooping 之后，MLD Snooping 功能只在属于该 VLAN 的端口上生效。

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。

表1-4 配置 MLD Snooping 版本

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

注意

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”。

1.4 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
- 配置相应端口组

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，如果在其老化时间超时前没有收到 MLD 普遍组查询报文或者 IPv6 PIM Hello 报文，AP 将把该端口从路由器端口列表中删除。

对于动态成员端口，如果在其老化时间超时前没有收到该 IPv6 组播组的 MLD 成员关系报告报文，AP 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。

1. 全局配置动态端口老化定时器

表1-5 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	**system-view**	-
进入MLD-Snooping视图	**mld-snooping**	-
配置动态路由器端口老化时间	**router-aging-time** *interval*	必选 缺省情况下，动态路由器端口的老化时间为260秒
配置动态成员端口老化时间	**host-aging-time** *interval*	必选 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1-6 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	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
配置动态路由器端口老化时间	**mld-snooping router-aging-time** *interval*	必选 缺省情况下，动态路由器端口的老化时间为260秒
配置动态成员端口老化时间	**mld-snooping host-aging-time** *interval*	必选 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。

表1-7 配置静态端口

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置静态成员端口		**mld-snooping static-group** *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*	必选 缺省情况下，端口不是静态成员端口

说明

- 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。
- 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

通常情况下，运行 MLD 的主机会对 MLD 查询器发出的查询报文进行响应。如果主机由于某种原因无法响应，就可能导致组播路由器认为该网段没有该 IPv6 组播组的成员，从而取消相应的转发路径。

为避免这种情况的发生，可以将 AP 的端口配置成为 IPv6 组播组成员（即配置模拟主机加入）。当收到 MLD 查询报文时由模拟主机进行响应，从而保证该 AP 能够继续收到 IPv6 组播报文。

模拟主机加入功能的实现原理如下：

- 在某端口上使能模拟主机加入功能时，AP 会通过该端口主动发送一个 MLD 成员关系报告报文；
- 在某端口上使能了模拟主机加入功能后，当收到 MLD 普遍组查询报文时，AP 会通过该端口响应一个 MLD 成员关系报告报文；
- 在某端口上关闭模拟主机加入功能时，AP 会通过该端口发送一个 MLD 离开组报文。

表1-8 配置模拟主机加入

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置模拟主机加入IPv6组播组或组播源组		**mld-snooping host-join** *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*	必选 缺省情况下，没有配置模拟主机加入IPv6组播组或组播源组

说明

- 每配置一次模拟主机加入，即相当于启动了一台独立的主机。例如，当收到 MLD 查询报文时，每条配置所对应的模拟主机将分别进行响应。
- 与静态成员端口不同，配置了模拟主机加入的端口会作为动态成员端口而参与动态成员端口的老化过程。

1.4.5 配置端口快速离开

端口快速离开是指当 AP 从某端口收到主机发送的离开某 IPv6 组播组的 MLD 离开组报文时，直接把该端口从对应转发表项的出端口列表中删除。此后，当 AP 收到对该 IPv6 组播组的 MLD 特定组查询报文时，AP 将不再向该端口转发。

在 AP 上，在只连接有一个接收者的端口上，可以通过使能端口快速离开功能来节约带宽和资源；而在连接有多个接收者的端口上，如果 AP 或该端口所在的 VLAN 已使能了丢弃未知 IPv6 组播数据报文功能，则不要再使能端口快速离开功能，否则，一个接收者的离开将导致该端口下属于同一 IPv6 组播组的其它接收者无法收到 IPv6 组播数据。

1. 全局配置端口快速离开

表1-9 全局配置端口快速离开

操作	命令	说明
进入系统视图	**system-view**	-
进入MLD-Snooping视图	**mld-snooping**	-

操作	命令	说明
使能端口快速离开功能	**fast-leave** [**vlan** *vlan-list*]	必选 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1-10 在端口上配置端口快速离开

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
使能端口快速离开功能		**mld-snooping fast-leave** [**vlan** *vlan-list*]	必选 缺省情况下，端口快速离开功能处于关闭状态

1.4.6 禁止端口成为动态路由器端口

目前，在 IPv6 组播用户接入网络中存在以下问题：

- 如果 AP 收到了某用户主机发来的 MLD 普遍组查询报文或 IPv6 PIM Hello 报文，那么该主机所在的端口就将成为动态路由器端口，从而使 VLAN 内的所有 IPv6 组播报文都会向该端口转发，导致该用户主机收到的 IPv6 组播报文失控。
- 同时，用户主机发送 MLD 普遍组查询报文或 IPv6 PIM Hello 报文，也会影响该接入网络中三层设备上的 IPv6 组播路由协议状态（如影响 MLD 查询器或 DR 的选举），严重时可能导致网络中断。

当禁止某端口成为动态路由器端口后，即使该端口收到了 MLD 普遍组查询报文或 IPv6 PIM Hello 报文，该端口也不会成为动态路由器端口，从而能够有效解决上述问题，提高网络的安全性和对 IPv6 组播用户的控制能力。

表1-11 禁止端口成为动态路由器端口

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
禁止端口成为动态路由器端口		**mld-snooping router-port-deny** [**vlan** *vlan-list*]	必选 缺省情况下，不禁止端口成为动态路由器端口

说明

本配置与静态路由器端口的配置互不影响。

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：

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

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。

1. 在VLAN内使能MLD Snooping查询器

表1-12 在 VLAN 内使能 MLD Snooping 查询器

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

注意

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 IPv6 组播网络中，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”。

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发送 MLD 普遍组查询报文的时间间隔。

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，所配置的发送 MLD 特定组查询报文的时间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发送 MLD 特定组查询报文的时间间隔相同。

1. 全局配置MLD查询和响应

表1-13 全局配置 MLD 查询和响应

操作	命令	说明
进入系统视图	**system-view**	-
进入MLD-Snooping视图	**mld-snooping**	-
配置MLD普遍组查询的最大响应时间	**max-response-time** *interval*	必选 缺省情况下，MLD普遍组查询的最大响应时间为10秒
配置发送MLD特定组查询报文的时间间隔	**last-listener-query-interval** *interval*	必选 缺省情况下，发送MLD特定组查询报文的时间间隔为1秒

2. 在VLAN内配置MLD查询和响应

表1-14 在 VLAN 内配置 MLD 查询和响应

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-

操作	命令	说明
配置发送MLD普遍组查询报文的时间间隔	**mld-snooping query-interval** *interval*	必选 缺省情况下，发送MLD普遍组查询报文的时间间隔为125秒
配置MLD普遍组查询的最大响应时间	**mld-snooping max-response-time** *interval*	必选 缺省情况下，MLD普遍组查询的最大响应时间为10秒
配置发送MLD特定组查询报文的时间间隔	**mld-snooping last-listener-query-interval** *interval*	必选 缺省情况下，发送MLD特定组查询报文的时间间隔为1秒

注意

应确保发送 MLD 普遍组查询报文的时间间隔大于 MLD 普遍组查询的最大响应时间，否则有可能造成对 IPv6 组播组成员的误删。

1.5.4 配置MLD查询报文源IPv6 地址

可以通过此项配置改变 MLD 查询报文的源 IPv6 地址。

1. 在VLAN内配置MLD查询报文源IPv6 地址

表1-15 在 VLAN 内配置 MLD 查询报文源 IPv6 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
配置MLD普遍组查询报文源IPv6地址	**mld-snooping general-query source-ip** { *ipv6-address* | **current-interface** }	必选 缺省情况下，MLD普遍组查询报文的源IPv6地址为FE80::02FF:FFFF:FE00:0001
配置MLD特定组查询报文源IPv6地址	**mld-snooping special-query source-ip** { *ipv6-address* | **current-interface** }	必选 缺省情况下，MLD特定组查询报文的源IPv6地址为FE80::02FF:FFFF:FE00:0001

注意

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

1.6 配置MLD Snooping策略

1.6.1 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 IPv6 ACL 规则
- 端口加入的 IPv6 组播组最大数量
- MLD 报文的 802.1p 优先级

1.6.2 配置IPv6 组播组过滤器

在使能了 MLD Snooping 的 AP 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 AP 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 AP 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。

1. 全局配置IPv6 组播组过滤器

表1-16 全局配置 IPv6 组播组过滤器

操作	命令	说明
进入系统视图	**system-view**	-
进入MLD-Snooping视图	**mld-snooping**	-
配置IPv6组播组过滤器	**group-policy** *acl6-number* [**vlan** *vlan-list*]	必选 缺省情况下，没有配置全局IPv6组播组过滤器，即各VLAN内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1-17 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		**system-view**	-
进入相应视图	进入二层以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置IPv6组播组过滤器		**mld-snooping group-policy** *acl6-number* [**vlan** *vlan-list*]	必选 缺省情况下，端口上没有配置IPv6组播组过滤器，即该端口下的主机可以加入任意合法的IPv6组播组

1.6.3 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，AP将丢弃所有收到的未知IPv6组播数据报文；
- 当关闭了丢弃未知 IPv6 组播数据报文功能时，AP 将在未知 IPv6 组播数据报文所属的 VLAN 内广播该报文。

1. 全局配置丢弃未知IPv6 组播数据报文

表1-18 全局配置丢弃未知 IPv6 组播数据报文

操作	命令	说明
进入系统视图	**system-view**	-
进入MLD-Snooping视图	**mld-snooping**	-
使能丢弃未知IPv6组播数据报文功能	**drop-unknown**	必选 缺省情况下，丢弃未知IPv6组播数据报文的功能处于关闭状态，即对未知IPv6组播数据报文进行广播

2. 在VLAN内配置丢弃未知IPv6 组播数据报文

表1-19 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	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
使能丢弃未知IPv6组播数据报文功能	**mld-snooping** **drop-unknown**	必选 缺省情况下，丢弃未知IPv6组播数据报文的功能处于关闭状态，即对未知IPv6组播数据报文进行广播

说明

对于同时支持 **drop-unknown** 和 **mld-snooping drop-unknown** 这两条命令的设备来说，MLD-Snooping 视图和 VLAN 视图下的配置是互斥的。也就是说，当在 MLD-Snooping 视图下全局使能了丢弃未知 IPv6 组播数据报文的功能后，不允许在 VLAN 视图下使能或关闭该功能，反之亦然。

1.6.4 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1-20 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	**system-view**	-
进入MLD-Snooping视图	**mld-snooping**	-
使能MLD成员关系报告报文抑制功能	**report-aggregation**	必选 缺省情况下，MLD成员关系报告报文抑制功能处于使能状态

1.6.5 配置端口加入的IPv6 组播组最大数量

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1-21 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		**system-view**	-
进入相应视图	进入二层以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口加入的IPv6组播组最大数量		**mld-snooping group-limit** *limit* [**vlan** *vlan-list*]	必选 缺省情况下，端口加入的IPv6组播组最大数量与设备的型号有关，请以设备的实际情况为准

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。其中，如果该端口已配置为静态成员端口，系统会将静态成员端口的配置重新生效一次；如果在该端口上配置了模拟主机加入，系统在收到模拟主机发来的报告报文之后才会重新建立相应的转发表项。

1.6.6 配置IPv6 组播组替换

由于某些特殊的原因，当前 AP 或端口上通过的 IPv6 组播组数目有可能会超过 AP 或该端口的限定；另外，在某些特定的应用中，AP 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 AP 或者某些端口上使能 IPv6 组播组替换功能。当 AP 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。

1. 全局配置IPv6 组播组替换

表1-22 全局配置 IPv6 组播组替换

操作	命令	说明
进入系统视图	**system-view**	-
进入MLD-Snooping视图	**mld-snooping**	-
使能IPv6组播组替换功能	**overflow-replace** [**vlan** *vlan-list*]	必选 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

表1-23 在端口上配置 IPv6 组播组替换

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入二层以太网或二层聚合接口视图	**interface** *interface-type interface-number*	二者必选其一
	进入端口组视图	**port-group manual** *port-group-name*	
使能IPv6组播组替换功能		**mld-snooping overflow-replace** [**vlan** *vlan-list*]	必选 缺省情况下，IPv6组播组替换功能处于关闭状态

注意

当端口加入的IPv6 组播组最大数量取缺省值时，IPv6 组播组替换功能将不会生效，因此在使能IPv6 组播组替换功能之前，必须先将端口通过的IPv6 组播组最大数量配置为非缺省值（具体配置过程请参见“1.6.5 配置端口加入的IPv6 组播组最大数量”）。

1.6.7 配置MLD报文的 802.1p优先级

可以通过本配置来改变 MLD 报文的 802.1p 优先级。当 AP 的出端口发生拥塞时，AP 通过识别报文的 802.1p 优先级，优先发送优先级较高的报文。

1. 全局配置MLD报文的 802.1p优先级

表1-24 全局配置 MLD 报文的 802.1p 优先级

操作	命令	说明
进入系统视图	**system-view**	-
进入MLD-Snooping视图	**mld-snooping**	-
配置MLD报文的802.1p优先级	**dot1p-priority** *priority-number*	必选 缺省情况下，MLD报文的802.1p优先级为0

2. 在VLAN内配置MLD报文的 802.1p优先级

表1-25 在 VLAN 内配置 MLD 报文的 802.1p 优先级

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
配置MLD报文的802.1p优先级	**mld-snooping dot1p-priority** *priority-number*	必选 缺省情况下，MLD报文的802.1p优先级为0

1.6.8 配置MLD Snooping主机跟踪功能

通过使能 MLD Snooping 主机跟踪功能，可以使 AP 能够记录正在接收 IPv6 组播数据的成员主机信息（包括主机的 IPv6 地址、运行时间和超时时间等），以便于网络管理员对这些主机进行监控和管理。

1. 全局配置MLD Snooping主机跟踪功能

表1-26 全局配置 MLD Snooping 主机跟踪功能

操作	命令	说明
进入系统视图	**system-view**	-
进入MLD-Snooping视图	**mld-snooping**	-
全局使能MLD Snooping主机跟踪功能	**host-tracking**	必选 缺省情况下，MLD Snooping主机跟踪功能处于关闭状态

2. 在VLAN内配置MLD Snooping主机跟踪功能

表1-27 在 VLAN 内配置 MLD Snooping 主机跟踪功能

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入VLAN视图	**vlan** *vlan-id*	-
在VLAN内使能MLD Snooping主机跟踪功能	**mld-snooping host-tracking**	必选 缺省情况下，MLD Snooping主机跟踪功能处于关闭状态

1.7 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 IPv6 组播组信息。

表1-28 MLD Snooping 显示和维护

配置	命令
查看MLD Snooping组的信息	**display mld-snooping group** [**vlan** *vlan-id*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看MLD Snooping跟踪的主机信息	**display mld-snooping host vlan** *vlan-id* **group** *ipv6-group-address* [**source** *ipv6-source-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看MLD Snooping监听到的MLD报文的统计信息	**display mld-snooping statistics** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除MLD Snooping组的动态加入记录	**reset mld-snooping group** { *ipv6-group-address* | **all** } [**vlan** *vlan-id*]
清除MLD Snooping监听到的所有MLD报文的统计信息	**reset mld-snooping statistics**

1.8 MLD Snooping典型配置举例

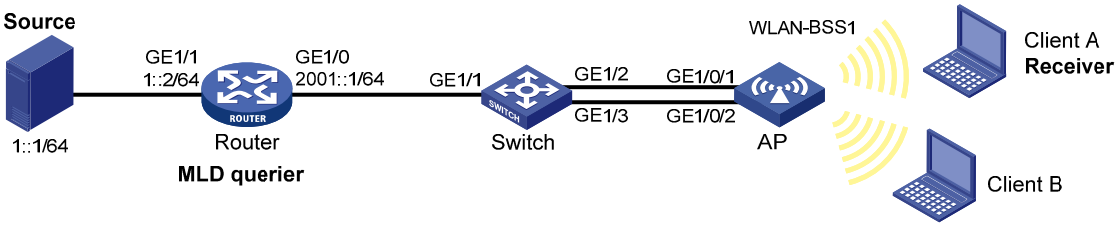
1.8.1 IPv6 组策略配置举例

1. 组网需求

- 如 图 1-3 所示，Router通过GigabitEthernet 1/1 接口连接IPv6 组播源（Source），通过GigabitEthernet 1/0 接口连接AP；
- Router 上运行 MLDv1，Swithc 和 AP 上运行版本 1 的 MLD Snooping，并由 Router 充当 MLD 查询器；
- 通过配置，使连接在 AP 上的接收者（Client）只能接收发往 IPv6 组播组 FF1E::101 的 IPv6 组播数据；

2. 组网图

图1-3 IPv6 组策略配置组网图



3. 配置步骤

(1) 使能 IPv6 转发功能，并配置 IPv6 地址

使能各设备的IPv6 转发功能，并按照 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

使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-DM，并在接口 GigabitEthernet 1/0 上使能 MLD。

```
<Router> system-view
[Router] multicast ipv6 routing-enable
[Router] interface GigabitEthernet 1/0
[Router-GigabitEthernet1/0] mld enable
[Router-GigabitEthernet1/0] pim ipv6 dm
[Router-GigabitEthernet1/0] quit
[Router] interface GigabitEthernet 1/1
[Router-GigabitEthernet1/1] pim ipv6 dm
[Router-GigabitEthernet1/1] quit
```

(3) 配置 Switch

全局使能 MLD Snooping。

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

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

```
[Switch] vlan 100
[Switch-vlan100] port GigabitEthernet 1/1 to GigabitEthernet 1/3
[Switch-vlan100] mld-snooping enable
[Switch-vlan100] quit
```

创建二层聚合端口 1。

```
[Switch] interface Bridge-Aggregation 1
[Switch-Bridge-Aggregation1] quit
```

分别将端口 GigabitEthernet 1/2 至 GigabitEthernet 1/3 加入到聚合组 1 中。

```
[Switch] interface GigabitEthernet 1/2
[Switch-GigabitEthernet1/2] port link-aggregation group 1
[Switch-GigabitEthernet1/2] quit
[Switch] interface GigabitEthernet 1/3
[Switch-GigabitEthernet1/3] port link-aggregation group 1
[Switch-GigabitEthernet1/3] quit
```

配置二层聚合接口 1 为 Trunk 端口，并允许 VLAN 100 的报文通过。

```
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] port link-type trunk
[Switch-Bridge-Aggregation1] port trunk permit vlan 100
```

将二层聚合口配置为 MLD Snooping 静态路由端口。

```
[Switch-Bridge-Aggregation1] mld-snooping static-router-port vlan 100
[Switch-Bridge-Aggregation1] quit
```

(4) 配置 AP

全局使能 MLD Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 WLAN-BSS1 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。

```
[AP] vlan 100
[AP-vlan100] port GigabitEthernet 1/0/1
[AP-vlan100] port GigabitEthernet 1/0/2
[AP-vlan100] port WLAN-BSS1
[AP-vlan100] mld-snooping enable
[AP-vlan100] mld-snooping drop-unknown
[AP-vlan100] quit
```

创建二层聚合端口 1。

```
[AP] interface Bridge-Aggregation 1
[AP-Bridge-Aggregation1] quit
```

分别将端口 GigabitEthernet 1/0/1 至 GigabitEthernet 1/0/2 加入到聚合组 1 中。

```
[AP] interface GigabitEthernet 1/0/1
[AP-GigabitEthernet1/0/1] port link-aggregation group 1
[AP-GigabitEthernet1/0/1] quit
[AP] interface GigabitEthernet 1/0/2
[AP-GigabitEthernet1/0/2] port link-aggregation group 1
[AP-GigabitEthernet1/0/2] quit
```

配置二层聚合接口 1 为 Trunk 端口，并允许 VLAN 100 的报文通过。

```
[AP] interface bridge-aggregation 1
[AP-Bridge-Aggregation1] port link-type trunk
[AP-Bridge-Aggregation1] port trunk permit vlan 100
```

配置 IPv6 组播组过滤器，使 VLAN 100 内的主机只能加入 IPv6 组播组 FF1E::101。

```
[AP] acl ipv6 number 2001
[AP-acl6-basic-2001] rule permit source ff1e::101 128
[AP-acl6-basic-2001] quit
[AP] mld-snooping
[AP–mld-snooping] group-policy 2001 vlan 100
[AP–mld-snooping] quit
```

(5) 检验配置效果

当配置完成后，Client 发送组地址为 FF1E::101 的 MLD 加入报文，通过使用 **display mld-snooping group** 命令可以查看 MLD Snooping 组播组的详细信息。

```
[AP] display mld-snooping group vlan 100
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Port flags: D-Dynamic port, S-Static port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 1 port(s).
            BAGG1                (D) ( 00:01:23 )
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:FF1E::101
        (::, FF1E::101):
          Host port(s):total 1 port(s).
            WLAN-BSS1               (D)
    MAC group(s):
      MAC group address:3333-0000-0101
          Host port(s):total 1 port.
            WLAN-BSS1
```

由此可见，AP 上的端口 WLAN-BSS1 已经加入了 IPv6 组播组 FF1E::101，VLAN 100 内没有其它组播组，并且 Client A 可以接收组播组 FF1E::101 的组播数据。

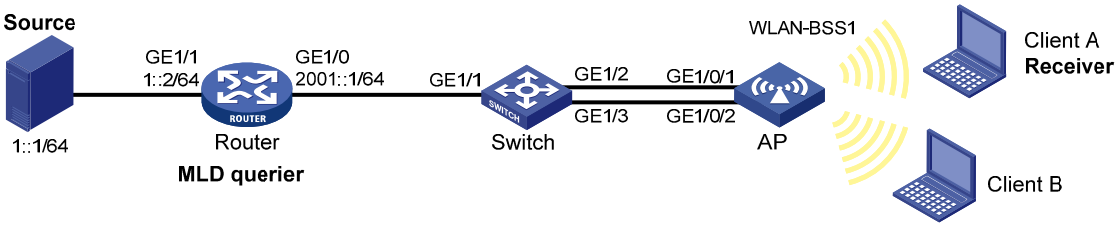
1.8.2 静态端口配置举例

1. 组网需求

- 如 图 1-4 所示，Router通过GigabitEthernet 1/1 接口连接组播源（Source），通过GigabitEthernet 1/0 接口连接Switch，Switch和AP之间配置链路聚合；
- Router 上运行 MLDv1，Switch 和 AP 上运行版本 1 的 MLD Snooping，并由 Router 充当 MLD 查询器；
- 通过在 AP 上配置静态成员端口，使无线客户端 Client 上不需要通过组播客户端软件加入组播组 ff1e::101 即可接收组播数据。

2. 组网图

图1-4 静态端口配置组网图



3. 配置步骤

(1) 使能 IPv6 转发功能，并配置 IPv6 地址

使能各设备的IPv6 转发功能，并按照 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

使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-DM，并在接口 GigabitEthernet 1/0 上使能 MLD。

```
<Router> system-view
[Router] multicast ipv6 routing-enable
[Router] interface GigabitEthernet 1/0
[Router-GigabitEthernet1/0] mld enable
[Router-GigabitEthernet1/0] pim ipv6 dm
[Router-GigabitEthernet1/0] quit
[Router] interface GigabitEthernet 1/1
[Router-GigabitEthernet1/1] pim ipv6 dm
[Router-GigabitEthernet1/1] quit
```

(3) 配置 Switch

全局使能 MLDSnooping。

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

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

```
[Switch] vlan 100
[Switch-vlan100] port GigabitEthernet 1/1 to GigabitEthernet 1/3
[Switch-vlan100] mld-snooping enable
[Switch-vlan100] quit
```

创建二层聚合端口 1。

```
[Switch] interface Bridge-Aggregation 1
[Switch-Bridge-Aggregation1] quit
```

分别将端口 GigabitEthernet 1/2 至 GigabitEthernet 1/3 加入到聚合组 1 中。

```
[Switch] interface GigabitEthernet 1/2
[Switch-GigabitEthernet1/2] port link-aggregation group 1
[Switch-GigabitEthernet1/2] quit
[Switch] interface GigabitEthernet 1/3
[Switch-GigabitEthernet1/3] port link-aggregation group 1
[Switch-GigabitEthernet1/3] quit
```

配置二层聚合接口 1 为 Trunk 端口，并允许 VLAN 100 的报文通过。

```
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] port link-type trunk
[Switch-Bridge-Aggregation1] port trunk permit vlan 100
```

将二层聚合口配置为 MLD Snooping 静态路由端口。

```
[Switch-Bridge-Aggregation1] mld-snooping static-router-port vlan 100
[Switch-Bridge-Aggregation1] quit
```

(4) 配置 AP

全局使能 MLD Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、WLAN-BSS1 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并使能丢弃未知组播数据报文功能。

```
[AP] vlan 100
[AP-vlan100] port GigabitEthernet 1/0/1
[AP-vlan100] port GigabitEthernet 1/0/2
[AP-vlan100] port WLAN-BSS1
[AP-vlan100] mld-snooping enable
[AP-vlan100] mld-snooping drop-unknown
[AP-vlan100] quit
```

创建二层聚合端口 1。

```
[AP] interface Bridge-Aggregation 1
[AP-Bridge-Aggregation1] quit
```

分别将端口 GigabitEthernet 1/0/1 至 GigabitEthernet 1/0/2 加入到聚合组 1 中。

```
[AP] interface GigabitEthernet 1/0/1
[AP-GigabitEthernet1/0/1] port link-aggregation group 1
[AP-GigabitEthernet1/0/1] quit
[AP] interface GigabitEthernet 1/0/2
[AP-GigabitEthernet1/0/2] port link-aggregation group 1
[AP-GigabitEthernet1/0/2] quit
```

配置二层聚合接口 1 为 Trunk 端口，并允许 VLAN 100 的报文通过。

```
[AP] interface bridge-aggregation 1
[AP-Bridge-Aggregation1] port link-type trunk
[AP-Bridge-Aggregation1] port trunk permit vlan 100
```

将二层聚合口配置为 MLD Snooping 静态成员端口。

```
[AP-Bridge-Aggregation1] mld-snooping static-group ff1e::101 vlan 100
[AP-Bridge-Aggregation1] quit
```

(5) 检验配置效果

查看 AP 上 VLAN 100 内 MLD Snooping 组的详细信息。

```
[AP] display mld-snooping group vlan 100 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:FF1E::101
        (::, FF1E::101):
          Attribute:    Host Port
          Host port(s):total 1 port(s).
            BAGG1                (S)
    MAC group(s):
      MAC group address:3333-0000-0101
```

```
Host port(s):total 1 port(s).
  BAGG1                (S)
```

由此可见，AP 上的二层聚合端口 BAGG1 已经成为了静态成员器端口。

1.9 常见配置错误举例

1.9.1 AP不能实现二层组播

1. 故障现象

AP 不能实现 MLD snooping 二层组播功能。

2. 分析

MLD Snooping 没有使能。

3. 处理过程

(1) 使用 **display current-configuration** 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。

1.9.2 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. 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 current-configuration** 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 **drop-unknown** 或 **mld-snooping drop-unknown** 命令使能丢弃未知 IPv6 组播数据报文功能。