H3C S5130S-SI[LI]&S5120V2-SI[LI]&S5110V2-SI&S5000V3-EI&S5000E-X&S3100V3-SI 系列以太网交换机

IP 组播配置指导

新华三技术有限公司
http://www.h3c.com

资料版本：6W103-20190822
产品版本：Release 612x 系列

前 言

本配置指导主要介绍组播业务的相关协议原理和具体配置，包括 IPv4 组播业务配置及 IPv6 组播业务的配置。利用组播技术可以实现网络中点到多点的高效数据传送。

前言部分包含如下内容：

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

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。

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 组播概述

1.1 组播简介

作为一种与单播（Unicast）和广播（Broadcast）并列的通信方式，组播（Multicast）技术能够有效地解决单点发送、多点接收的问题，从而实现了网络中点到多点的高效数据传送，能够节约大量网络带宽、降低网络负载。

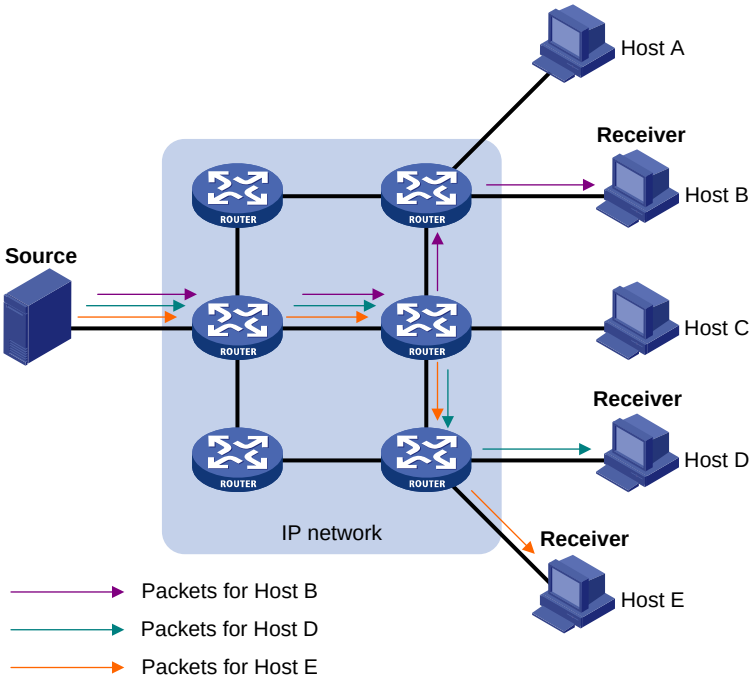
利用组播技术可以方便地提供一些新的增值业务，包括在线直播、网络电视、远程教育、远程医疗、网络电台、实时视频会议等对带宽和数据交互的实时性要求较高的信息服务。

1.1.1 三种信息传输方式的比较

1. 单播方式的信息传输

如 图 1-1 所示，在IP网络中若采用单播的方式，信息源（即Source）要为每个需要信息的主机（即Receiver）都发送一份独立的信息拷贝。

图1-1 单播方式的信息传输



假设 Host B、Host D 和 Host E 需要信息，则 Source 要与 Host B、Host D 和 Host E 分别建立一条独立的信息传输通道。

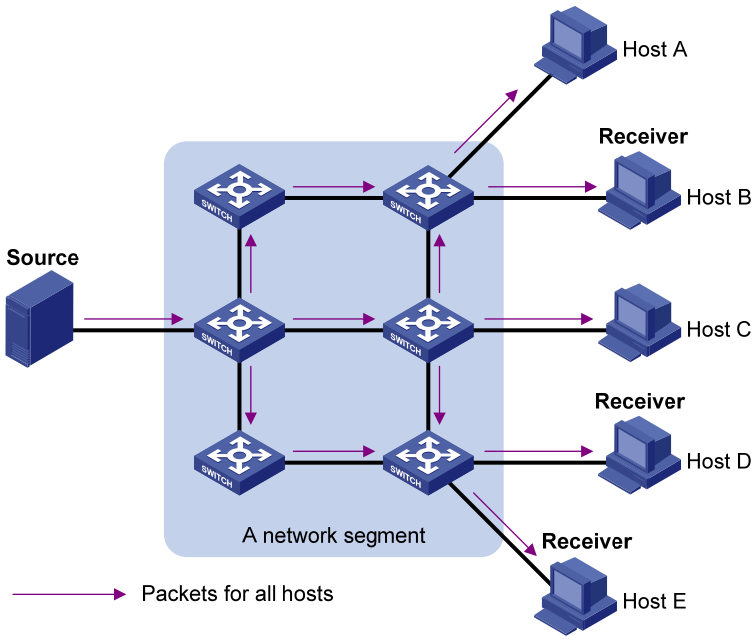
采用单播方式时，网络中传输的信息量与需要该信息的用户量成正比，因此当需要该信息的用户数量较大时，信息源需要将多份内容相同的信息发送给不同的用户，这对信息源以及网络带宽都将造成巨大的压力。

从单播方式的信息传播过程可以看出，该传输方式不利于信息的批量发送。

2. 广播方式的信息传输

如 图 1-2 所示，在一个网段中若采用广播的方式，信息源（即Source）将把信息传送给该网段中的所有主机，而不管其是否需要该信息。

图1-2 广播方式的信息传输



假设只有 Host B、Host D 和 Host E 需要信息，若将该信息在网段中进行广播，则原本不需要信息的 Host A 和 Host C 也将收到该信息，这样不仅信息的安全性得不到保障，而且会造成同一网段中信息的泛滥。

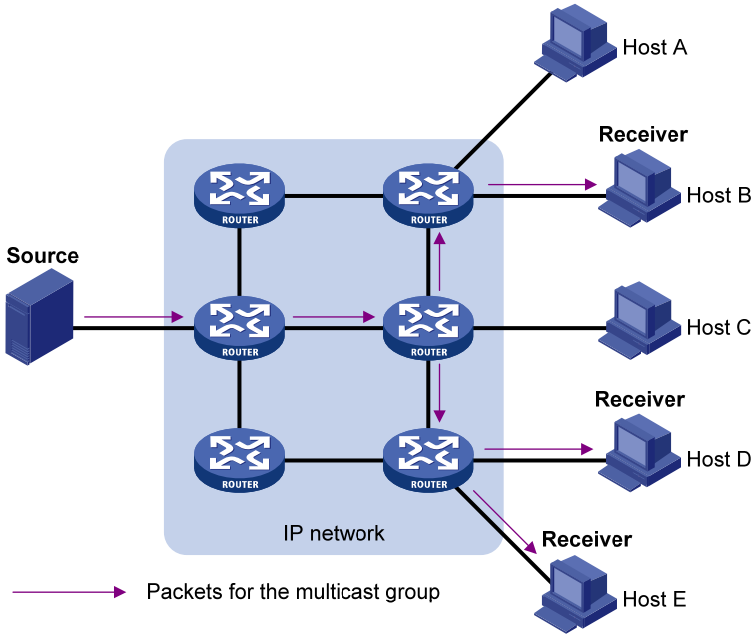
因此，广播方式不利于与特定对象进行数据交互，并且还浪费了大量的带宽。

3. 组播方式的信息传输

综上所述，传统的单播和广播的通信方式均不能以最小的网络开销实现单点发送、多点接收的问题，IP 组播技术的出现及时解决了这个问题。

如 图 1-3 所示，当IP网络中的某些主机（即Receiver）需要信息时，若采用组播的方式，组播源（即Source）仅需发送一份信息，借助组播路由协议建立组播分发树，被传递的信息在距离组播源尽可能远的网络节点才开始复制和分发。

图1-3 组播方式的信息传输



假设只有 Host B、Host D 和 Host E 需要信息，采用组播方式时，可以让这些主机加入同一个组播组（Multicast group），组播源向该组播组只需发送一份信息，并由网络中各路由器根据该组播组中各成员的分布情况对该信息进行复制和转发，最后该信息会准确地发送给 Host B、Host D 和 Host E。

综上所述，组播的优势归纳如下：

- 相比单播来说，组播的优势在于：由于被传递的信息在距信息源尽可能远的网络节点才开始被复制和分发，所以用户的增加不会导致信息源负载的加重以及网络资源消耗的显著增加。
- 相比广播来说，组播的优势在于：由于被传递的信息只会发送给需要该信息的接收者，所以不会造成网络资源的浪费，并能提高信息传输的安全性；另外，广播只能在同一网段中进行，而组播可以实现跨网段的传输。

1.1.2 组播传输的特点

组播传输的特点归纳如下：

- “组播组”是一个用 IP 组播地址进行标识的接收者集合，主机通过加入某组播组成为该组播组的成员，从而可以接收发往该组播组的组播数据。组播源通常不需要加入组播组。
- 信息的发送者称为“组播源”，如 图 1-3 中的Source。一个组播源可以同时向多个组播组发送信息，多个组播源也可以同时向一个组播组发送信息。
- 所有加入某组播组的主机便成为该组播组的成员，如 图 1-3 中的Receiver。组播组中的成员是动态的，主机可以在任何时刻加入或离开组播组。组播组成员可以广泛地分布在网络中的任何地方。
- 支持三层组播功能的路由器或三层交换机统称为“组播路由器”或“三层组播设备”。组播路由器不仅能够提供组播路由功能，也能够在与用户连接的末梢网段上提供组播组成员的管理功能。组播路由器本身也可能是组播组的成员。

为了更好地理解，可以将组播方式的信息传输过程类比于电视节目的传送过程，如 表 1-1 所示。

表1-1 组播信息传输与电视节目传输的类比

步骤	电视节目的传送过程	组播方式的信息传输过程
1	电视台S通过频道G传送电视节目	组播源S向组播组G发送组播数据
2	用户U将电视机的频道调至频道G	接收者U加入组播组G
3	用户U能够收看到由电视台S通过频道G传送的电视节目了	接收者U能够收到由组播源S发往组播组G的组播数据了
4	用户U关闭电视机或切换到其它频道	接收者U离开组播组G

1.1.3 组播的优点和应用

1. 组播的优点

组播技术的优点主要在于：

- 提高效率：减轻信息源服务器和网络设备 CPU 的负荷；
- 优化性能：减少冗余流量；
- 分布式应用：使用最少的网络资源实现点到多点应用。

2. 组播的应用

组播技术主要应用于以下几个方面：

- 多媒体、流媒体的应用，如：网络电视、网络电台、实时视/音频会议；
- 培训、联合作业场合的通信，如：远程教育、远程医疗；
- 数据仓库、金融应用（股票）；
- 其它任何“点到多点”的数据发布应用。

1.2 组播模型分类

根据接收者对组播源处理方式的不同，组播模型分为 ASM、SFM 和 SSM。

1.2.1 ASM模型

简单地说，ASM（Any-Source Multicast，任意信源组播）模型就是任意源组播模型。

在 ASM 模型中，任意一个发送者都可以作为组播源向某个组播组地址发送信息，接收者通过加入由该地址标识的组播组，来接收发往该组播组的组播信息。

在 ASM 模型中，接收者无法预先知道组播源的位置，但可以在任意时间加入或离开该组播组。

1.2.2 SFM模型

SFM（Source-Filtered Multicast，信源过滤组播）模型继承了 ASM 模型，从发送者角度来看，两者的组播组成员关系完全相同。

SFM 模型在功能上对 ASM 模型进行了扩展。在 SFM 模型中，上层软件对收到的组播报文的源地址进行检查，允许或禁止来自某些组播源的报文通过。因此，接收者只能收到来自部分组播源的组播数据。从接收者的角度来看，只有部分组播源是有效的，组播源被经过了筛选。

1.2.3 SSM模型

在现实生活中，用户可能只对某些组播源发送的组播信息感兴趣，而不愿接收其它源发送的信息。SSM（Source-Specific Multicast，指定信源组播）模型为用户提供了一种能够在客户端指定组播源的传输服务。

SSM 模型与 ASM 模型的根本区别在于：SSM 模型中的接收者已经通过其它手段预先知道了组播源的具体位置。SSM 模型使用与 ASM/SFM 模型不同的组播地址范围，直接在接收者与其指定的组播源之间建立专用的组播转发路径。

1.3 组播地址

1.3.1 IP组播地址

1. IPv4 组播地址

IANA（Internet Assigned Numbers Authority，互联网编号分配委员会）将D类地址空间分配给IPv4组播使用，范围从 224.0.0.0 到 239.255.255.255，具体分类及其含义如 表 1-2 所示。

表1-2 IPv4 组播地址的范围及含义

地址范围	含义
224.0.0.0～224.0.0.255	永久组地址。除224.0.0.0保留不做分配外，其它地址供路由协议、拓扑查找和协议维护等使用，常用的永久组地址及其含义如表1-3所示。对于以该范围内组播地址为目的地址的数据包来说，不论其TTL（Time to Live，生存时间）值为多少，都不会被转发出本地网段
224.0.1.0～238.255.255.255	用户组地址，全网范围内有效。包含两种特定的组地址： • 232.0.0.0/8：SSM 组地址 • 233.0.0.0/8：GLOP 组地址
239.0.0.0～239.255.255.255	本地管理组地址，仅在本地管理域内有效。使用本地管理组地址可以灵活定义组播域的范围，以实现不同组播域之间的地址隔离，从而有助于在不同组播域内重复使用相同组播地址而不会引起冲突。详情请参见RFC 2365


说明

GLOP 是一种 AS（Autonomous System，自治系统）之间的组播地址分配机制，将 AS 号填入该范围内组播地址的中间两个字节中，每个 AS 都可以得到 255 个组播地址。有关 GLOP 的详细介绍请参见 RFC 2770。

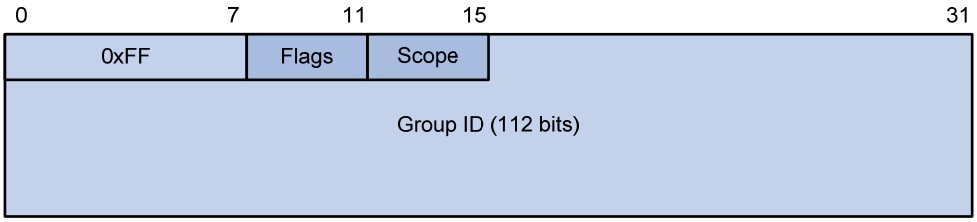
表1-3 常用永久组地址及其含义

永久组地址	含义
224.0.0.1	所有系统，包括主机与路由器
224.0.0.2	所有组播路由器
224.0.0.3	未分配

永久组地址	含义
224.0.0.4	DVMRP（Distance Vector Multicast Routing Protocol，距离矢量组播路由协议）路由器
224.0.0.5	OSPF（Open Shortest Path First，开放最短路径优先）路由器
224.0.0.6	OSPF指定路由器/备用指定路由器
224.0.0.7	ST（Shared Tree，共享树）路由器
224.0.0.8	ST主机
224.0.0.9	RIP-2（Routing Information Protocol version 2，路由信息协议版本2）路由器
224.0.0.11	移动代理
224.0.0.12	DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）服务器/中继代理
224.0.0.13	所有PIM（Protocol Independent Multicast，协议无关组播）路由器
224.0.0.14	RSVP（Resource Reservation Protocol，资源预留协议）封装
224.0.0.15	所有CBT（Core-Based Tree，有核树）路由器
224.0.0.16	指定SBM（Subnetwork Bandwidth Management，子网带宽管理）
224.0.0.17	所有SBM
224.0.0.18	VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）

2. IPv6 组播地址

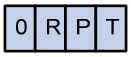
图1-4 IPv6 组播地址格式



如 图 1-4 所示，IPv6 组播地址中各字段的含义如下：

- 0xFF：最高 8 比特为 11111111，标识此地址为 IPv6 组播地址。

图1-5 Flags 字段格式



- Flags：4 比特，如 图 1-5 所示，该字段中各位的取值及含义如 表 1-4 所示。

表1-4 Flags 字段各位的取值及含义

位	取值及含义
0位	保留位，必须取0

位	取值及含义
R位	• 取 0 表示非内嵌 RP 的 IPv6 组播地址 • 取 1 则表示内嵌 RP 的 IPv6 组播地址（此时 P、T 位也必须置 1）
P位	• 取 0 表示非基于单播前缀的 IPv6 组播地址 • 取 1 则表示基于单播前缀的 IPv6 组播地址（此时 T 位也必须置 1）
T位	• 取 0 表示由 IANA 永久分配的 IPv6 组播地址 • 取 1 则表示非永久分配的 IPv6 组播地址

- Scope：4 比特，标识该IPv6 组播组的应用范围，其可能的取值及其含义如 表 1-5 所示。

表1-5 Scope 字段的取值及其含义

取值	含义
0、F	保留（Reserved）
1	接口本地范围（Interface-Local Scope）
2	链路本地范围（Link-Local Scope）
3	子网本地范围（Subnet-Local Scope）
4	管理本地范围（Admin-Local Scope）
5	站点本地范围（Site-Local Scope）
6、7、9～D	未分配（Unassigned）
8	机构本地范围（Organization-Local Scope）
E	全球范围（Global Scope）

- Group ID：112 比特，IPv6 组播组的标识号，用来在由 Scope 字段所指定的范围内唯一标识 IPv6 组播组。

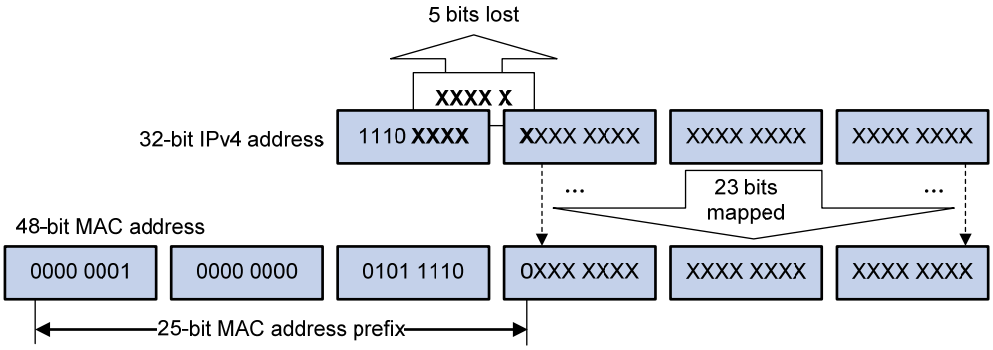
1.3.2 以太网组播MAC地址

以太网组播 MAC 地址用于在链路层上标识属于同一组播组的接收者。

1. IPv4 组播MAC地址

IANA规定，IPv4 组播MAC地址的高 24 位为 0x01005E，第 25 位为 0，低 23 位为IPv4 组播地址的低 23 位。IPv4 组播地址与MAC地址的映射关系如 图 1-6 所示。

图1-6 IPv4 组播地址与 MAC 地址的映射关系

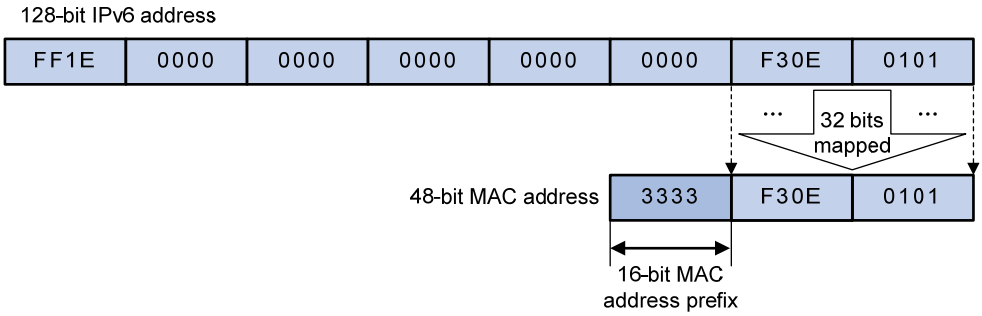


由于 IPv4 组播地址的高 4 位固定为 1110，而低 28 位中只有 23 位被映射到 IPv4 组播 MAC 地址上，从而导致有 5 位信息丢失。于是，将有 32 个 IPv4 组播地址被重复映射到同一个 IPv4 组播 MAC 地址上，因此设备在进行二层处理时，可能会收到一些本不需要的组播数据，这些多余的组播数据就需要上层进行过滤了。

2. IPv6 组播MAC地址

IANA规定，IPv6 组播MAC地址的高 16 位为 0x3333，低 32 位为IPv6 组播地址的低 32 位。如 图1-7 所示，是IPv6 组播地址FF1E::F30E:101 的MAC地址映射举例。从图中可见，由于IPv6 组播地址中只有低 32 位被映射到IPv6 组播MAC地址，因此也存在与IPv4 类似的地址重复映射问题。

图1-7 IPv6 组播地址的 MAC 地址映射举例



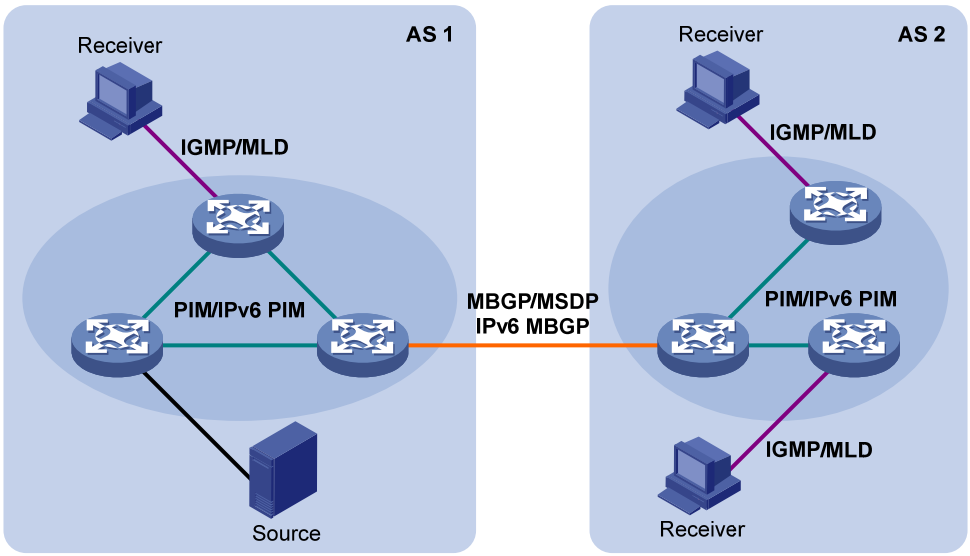
1.4 组播协议

通常，我们把工作在网络层的 IP 组播称为“三层组播”，相应的组播协议称为“三层组播协议”，包括 IGMP/MLD、PIM/IPv6 PIM、MSDP、MBGP/IPv6 MBGP 等；把工作在数据链路层的 IP 组播称为“二层组播”，相应的组播协议称为“二层组播协议”，包括 IGMP Snooping/MLD Snooping、PIM Snooping/IPv6 PIM Snooping、组播 VLAN/IPv6 组播 VLAN 等。其中，IGMP Snooping、PIM Snooping、组播 VLAN、IGMP、PIM、MSDP 和 MBGP 应用于 IPv4；MLD Snooping、IPv6 PIM Snooping、IPv6 组播 VLAN、MLD、IPv6 PIM 和 IPv6 MBGP 应用于 IPv6。本节主要针对二、三层组播协议在网络中的应用位置和功能进行总体介绍，有关各协议的详细介绍请参见“IP 组播配置指导”中的相关章节。

1.4.1 三层组播协议

三层组播协议包括组播组管理协议和组播路由协议两种类型，它们在网络中的应用位置如 图 1-8 所示。

图1-8 三层组播协议的应用位置



- 组播组管理协议

在主机和与其直接相连的三层组播设备之间通常采用组播组的管理协议 IGMP（Internet Group Management Protocol，互联网组管理协议）或 MLD（Multicast Listener Discovery Protocol，组播侦听者发现协议），该协议规定了主机与三层组播设备之间建立和维护组播组成员关系的机制。

- 组播路由协议

组播路由协议运行在三层组播设备之间，用于建立和维护组播路由，并正确、高效地转发组播数据包。组播路由建立了从一个数据源端到多个接收端的无环（loop-free）数据传输路径，即组播分发树。

对于 ASM 模型，可以将组播路由分为域内和域间两大类：

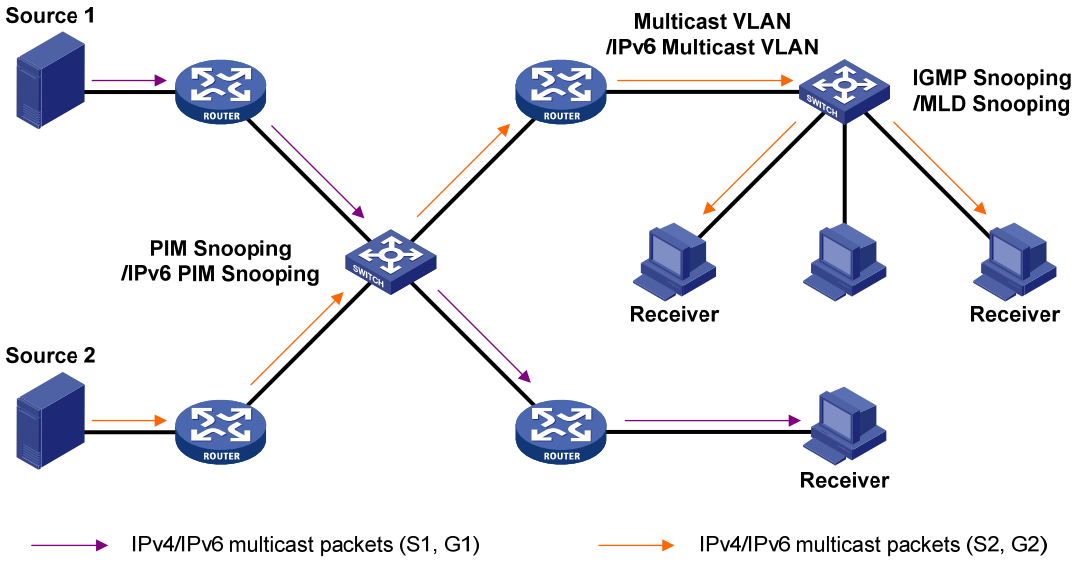
- 域内组播路由用来在 AS 内部发现组播源并构建组播分发树，从而将组播信息传递到接收者。在众多域内组播路由协议中，PIM（Protocol Independent Multicast，协议无关组播）是目前较为典型的一个。按照转发机制的不同，PIM 可以分为 DM（Dense Mode，密集模式）和 SM（Sparse Mode，稀疏模式）两种模式。
- 域间组播路由用来实现组播信息在 AS 之间的传递，目前比较成型的解决方案有：MSDP（Multicast Source Discovery Protocol，组播源发现协议）能够跨越 AS 传播组播源的信息；而 MP-BGP（Multiprotocol Border Gateway Protocol，多协议边界网关协议）的组播扩展 MBGP（Multicast BGP）则能够跨越 AS 传播组播路由。

对于 SSM 模型，没有域内和域间的划分。由于接收者预先知道组播源的具体位置，因此只需要借助 PIM-SM 构建的通道即可实现组播信息的传输。

1.4.2 二层组播协议

二层组播协议包括IGMP Snooping/MLD Snooping、PIM Snooping/IPv6 PIM Snooping、组播VLAN/IPv6 组播VLAN等，它们在网络中的应用位置如 图 1-9 所示。

图1-9 二层组播协议的应用位置



- IGMP Snooping/MLD Snooping

IGMP Snooping（Internet Group Management Protocol Snooping，互联网组管理协议窥探）和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 IGMP 或 MLD 报文来生成二层组播转发表，从而管理和控制组播数据报文的转发，实现组播数据报文在二层的按需分发。

- PIM Snooping/IPv6 PIM Snooping

PIM Snooping（Protocol Independent Multicast Snooping，协议无关组播窥探）或 IPv6 PIM Snooping 运行在二层设备上，通过与 IGMP Snooping 或 MLD Snooping 配合来对收到的 PIM 协议报文进行分析，将有接收需求的端口添加到 PIM Snooping 路由表或 IPv6 PIM Snooping 路由表的相应表项中，以实现组播报文的精确转发。

- 组播 VLAN/IPv6 组播 VLAN

在传统的组播点播方式下，当连接在二层设备上、属于不同 VLAN 的用户分别进行组播点播时，三层组播设备需要向该二层设备的每个 VLAN 分别发送一份组播数据；而当二层设备运行了组播 VLAN 或 IPv6 组播 VLAN 之后，三层组播设备只需向该二层设备的组播 VLAN 或 IPv6 组播 VLAN 发送一份组播数据即可，从而既避免了带宽的浪费，也减轻了三层组播设备的负担。

1.5 组播报文的转发机制

在组播模型中，IP 报文的目的地址字段为组播组地址，组播源向以此目的地址所标识的主机群组传送信息。因此，转发路径上的组播路由器为了将组播报文传送到各个方位的接收站点，往往需要将从一个入接口收到的组播报文转发到多个出接口。与单播模型相比，组播模型的复杂性就在于此：

- 为了保证组播报文在网络中的传输，必须依靠单播路由表、单独提供给组播使用的路由表（如 MBGP 路由表）或者组播静态路由来指导转发；
- 为了处理同一设备在不同接口上收到来自不同对端的相同组播信息，需要对组播报文的入接口进行 RPF（Reverse Path Forwarding，逆向路径转发）检查，以决定转发还是丢弃该报文。RPF 检查机制是大部分组播路由协议进行组播转发的基础。

有关 RPF 检查机制的详细介绍，请参见“IP 组播配置指导”中的“组播路由与转发”或“IPv6 组播路由与转发”。

1.6 组播框架结构

对于 IP 组播，需要关注下列问题：

- 组播源将组播信息传输到哪里？即组播寻址机制；
- 网络中有哪些接收者？即主机注册；
- 这些接收者需要从哪个组播源接收信息？即组播源发现；
- 组播信息如何传输？即组播路由。

IP 组播属于端到端的服务，组播机制包括以下四个部分：

- 寻址机制：借助组播地址，实现信息从组播源发送到一组接收者；
- 主机注册：利用组播组管理协议，允许接收者主机动态加入和离开某组播组，实现对组播成员的管理；
- 组播路由：利用组播路由协议，构建组播报文分发树（即组播数据在网络中的树型转发路径），并通过该分发树将报文从组播源传输到接收者；

组播应用：组播源与接收者必须安装支持视频会议等组播应用的软件，TCP/IP 协议栈必须支持组播信息的发送和接收。

1.7 组播中常用的表示法

在组播中，经常出现以下两种表示方式：

- （*，G）：通常用来表示共享树，或者由任意组播源发往组播组 G 的组播报文。其中的“*”代表任意组播源，“G”代表特定组播组 G。
- （S，G）：也称为“组播源组”，通常用来表示最短路径树，或者由组播源 S 发往组播组 G 的组播报文。其中的“S”代表特定组播源 S，“G”代表特定组播组 G。

目 录

1 IGMP Snooping

1.1 IGMP Snooping简介

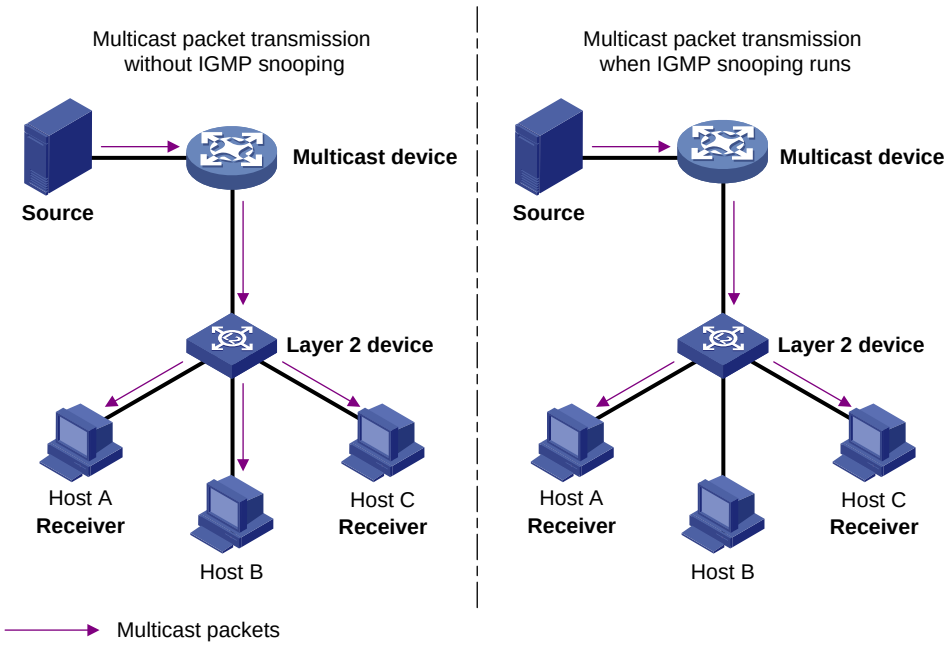
IGMP Snooping（Internet Group Management Protocol Snooping，互联网组管理协议窥探）运行在二层设备上，通过侦听三层设备与主机之间的 IGMP 报文来生成二层组播转发表，从而管理和控制组播数据报文的转发，实现组播数据报文在二层的按需分发。

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



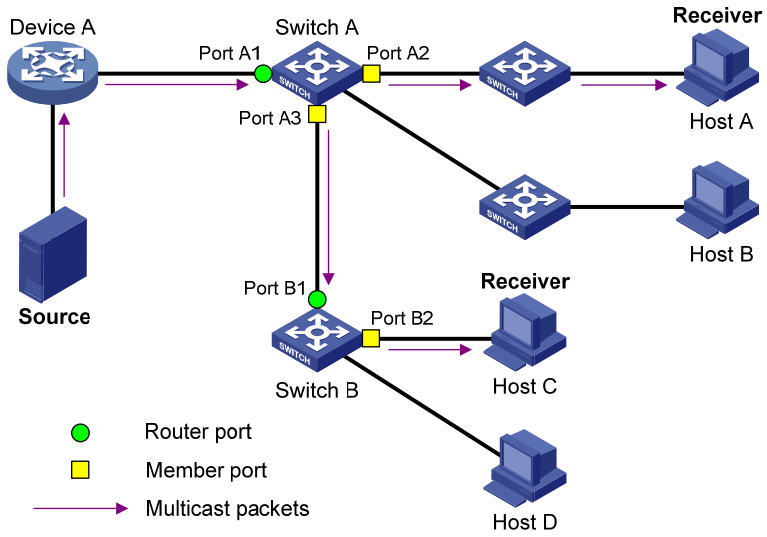
IGMP Snooping 通过二层组播将信息只转发给有需要的接收者，可以带来以下好处：

- 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端口分类

如 图 1-2 所示，Device A连接组播源，在Switch A和Switch B上分别运行IGMP Snooping，Host A和Host C为接收者主机（即组播组成员）。根据在网络中所处位置的不同，我们将IGMP Snooping端口分为路由器端口和成员端口两类，以下分别介绍。

图1-2 IGMP Snooping 端口示意图



1. 路由器端口

在运行了IGMP Snooping的二层设备上，朝向上游三层组播设备的端口称为路由器端口。如 图 1-2 中Switch A的Port A1 端口和Switch B的Port B1 端口。

根据来源不同，路由器端口可分为：

- 动态路由器端口：所有收到 IGMP 普遍组查询报文（源地址非 0.0.0.0）或 PIM Hello 报文的端口，都被维护为动态路由器端口。这些端口被记录在动态路由器端口列表中，每个端口都有一个老化定时器。在老化定时器超时前，动态路由器端口如果收到了 IGMP 普遍组查询报文（源地址非 0.0.0.0）或 PIM Hello 报文，该定时器将被重置；否则，该端口将被从动态路由器端口列表中删除。
- 静态路由器端口：通过命令行手工配置的路由器端口称为静态路由器端口，这些端口被记录在静态路由器端口列表中。静态路由器端口只能通过命令行手工删除，不会被老化。

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。如果没有特别指明，本文中提到的路由器端口包括动态路由器端口和静态路由器端口。

---

2. 成员端口

在运行了IGMP Snooping的二层设备上，朝向下游组播组成员的端口称为成员端口。如 图 1-2 中Switch A的Port A2 和 Port A3 端口，以及Switch B的Port B2 端口。

根据来源不同，成员端口也可分为：

- 动态成员端口：所有收到 IGMP 成员关系报告报文的端口，都被维护为动态成员端口。这些端口被记录在动态 IGMP Snooping 转发表中，每个端口都有一个老化定时器。在老化定时器超时前，动态成员端口如果收到了 IGMP 成员关系报告报文，该定时器将被重置；否则，该端口将被从动态 IGMP Snooping 转发表中删除。
- 静态成员端口：通过命令行手工配置的成员端口称为静态成员端口，这些端口被记录在静态 IGMP Snooping 转发表中。静态路由器端口只能通过命令行手工删除，不会被老化。

说明

如果没有特别指明，本文中提到的成员端口包括动态成员端口和静态成员端口。

1.1.3 IGMP Snooping工作机制

运行了 IGMP Snooping 的二层设备对不同 IGMP 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“1.7.2 配置静态成员端口”和“1.7.3 配置静态路由器端口”

1. 普遍组查询

IGMP 查询器定期向本地网段内的所有主机与设备（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，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：

- 如果在动态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。
- 如果在动态路由器端口列表中尚未包含该动态路由器端口，则将其添加到动态路由器端口列表中，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，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

二层设备不会将 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，从而使二层设备无法获知这些端口下还有该组播组的成员主机。

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，因此二层设备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，二层设备就会将该端口从相应转发表项的出端口列表中删除。

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，以通知三层组播设备自己离开了某个组播组。当二层设备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，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除该端口还有别的成员端口存在，二层设备不会向任何端口转发该报文，而将其直接丢弃。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，所以二层设备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，而是向该端口发送 IGMP 特定组查询报文，并根据 IGMP 特定组查询报文调整该端口的老化定时器（老化时间为 2×IGMP 特定组查询报文的发送间隔）；
- 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只有该端口，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组播组的其它成员，所以二层设备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，而是向该端口发送 IGMP 特定组查询报文，并根据 IGMP 特定组查询报文调整该端口的老化定时器（老化时间为 2×IGMP 特定组查询报文的发送间隔）。

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。二层设备在收到 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），二层设备在其老化时间内：

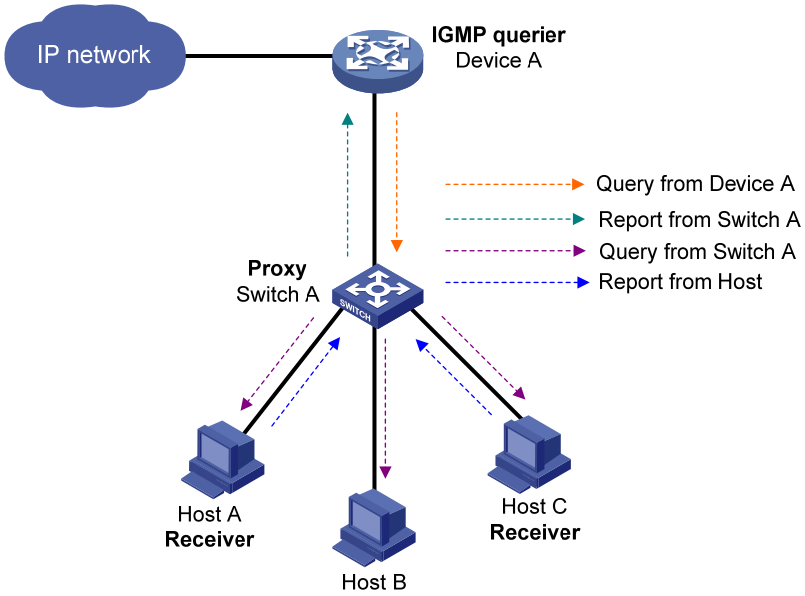
- 如果从该端口收到了主机响应该特定组查询的 IGMP 成员关系报告报文，则表示该端口下还有该组播组的成员，于是重置其老化定时器；
- 如果没有从该端口收到主机响应特定组查询的 IGMP 成员关系报告报文，则表示该端口下已没有该组播组的成员。当该端口的老化定时器超时后，将其从该组播组所对应转发表项的出端口列表中删除。

1.1.4 IGMP Snooping Proxy

为了减少上游设备收到的 IGMP 报告报文和离开报文的数量，可以通过在边缘设备上配置 IGMP Snooping Proxy（IGMP Snooping 代理）功能，使其能够代理下游主机向上游设备发送报告报文和

离开报文。配置了 IGMP Snooping Proxy 功能的设备称为 IGMP Snooping 代理设备，在其上游设备看来，它就相当于一台主机。但主机上的 IGMP 成员关系报告抑制机制在 IGMP Snooping 代理设备上并不会生效。

图1-3 IGMP Snooping Proxy 组网图



如 图 1-3 所示，作为IGMP Snooping代理设备的Switch A，对其上游的IGMP查询器Device A来说相当于一台主机，代理下游主机向Device A发送报告报文和离开报文。

IGMP Snooping代理设备对IGMP报文的处理方式如 表 1-1 所示。

表1-1 IGMP Snooping 代理设备对 IGMP 报文的处理方式

IGMP 报文	处理方式
普遍组查询报文	收到普遍组查询报文后，向本VLAN内除接收端口以外的所有端口转发；同时根据本地维护的组成员关系生成报告报文，并向所有路由器端口发送
特定组/特定源组查询报文	收到针对某组播组的特定组/特定源组查询报文时，向本VLAN内除接收端口以外的所有路由器端口转发；若该组对应的转发表项中还有成员端口，则向本VLAN内所有路由器端口回复该组的报告报文
报告报文	从某端口收到某组播组的报告报文时，若已存在该组对应的转发表项，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；若已存在该组对应的转发表项，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；若尚不存在该组对应的转发表项，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，然后向所有路由器端口发送该组的报告报文
离开报文	从某端口收到某组播组的离开报文后，向该端口发送针对该组的特定组查询报文。只有当删除某组播组对应转发表项中的最后一个成员端口时，才会向所有路由器端口发送该组的离开报文

1.1.5 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配置限制和指导

对于从 Secondary VLAN 中收到的主机加入请求，相关的 IGMP Snooping 转发表项都将维护在 Primary VLAN 中，因此IGMP Snooping功能只需在Primary VLAN中配置既可，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“Private VLAN”。

二层聚合接口与其各成员端口上的IGMP Snooping配置互不影响，且成员端口上的IGMP Snooping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 IGMP Snooping 配置也不会参与聚合计算。

对于既可在 VLAN 视图下配置，又可在 IGMP-Snooping 视图下对多个 VLAN 进行配置的功能，两个视图下配置的优先级相同，最新配置生效。

对于既可在 VLAN 视图下配置，又可在 IGMP-Snooping 视图下对所有 VLAN 配置的功能，VLAN 视图下的配置的优先级较高。

对于既可在接口视图下配置，又可在 IGMP-Snooping 视图下配置的功能，IGMP-Snooping 视图下的配置对指定 VLAN 内的所有端口生效，接口视图下配置只对当前接口生效，且接口视图下的配置优先级较高。

1.3 基于VLAN的IGMP Snooping配置任务简介

基于 VLAN 的 IGMP Snooping 配置任务如下：

(1) 开启设备的IGMP Snooping特性

(2) 使能IGMP Snooping

请至少选择以下一项任务进行配置：

- 使能全局IGMP Snooping
- 使能VLAN的IGMP Snooping

(3) （可选）配置IGMP Snooping基本功能

- 配置IGMP Snooping版本
- 配置IGMP Snooping转发表项的全局最大数量
- 配置静态组播MAC地址表项
- 配置IGMP特定组查询报文的发送间隔

(4) （可选）配置IGMP Snooping端口功能

- 配置动态端口老化定时器
- 配置静态成员端口
- 配置静态路由器端口
- 配置模拟主机加入
- 配置端口快速离开功能
- 禁止端口成为动态路由器端口

(5) （可选）配置IGMP Snooping查询器

- 开启IGMP Snooping查询器
- 开启IGMP Snooping查询器选举功能
- 配置IGMP普遍组查询和响应

(6) （可选）配置IGMP Snooping Proxy

(7) （可选）调整IGMP报文

- 配置IGMP报文的源IP地址
- 配置IGMP报文的 802.1p优先级

(8) （可选）配置IGMP Snooping策略

- 配置组播组过滤器
- 配置组播数据报文源端口过滤
- 配置丢弃未知组播数据报文
- 配置IGMP成员关系报告报文抑制
- 配置端口加入的组播组最大数量
- 配置组播组替换功能
- 配置IGMP Snooping主机跟踪功能
- 配置组播用户控制策略

(9) （可选）配置设备发送的IGMP协议报文的DSCP优先级

1.4 开启设备的IGMP Snooping特性

1. 功能简介

只有在开启了设备的 IGMP Snooping 特性后，才能进行其它的 IGMP Snooping 相关配置。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启设备的 IGMP Snooping 特性，并进入 IGMP-Snooping 视图。

igmp-snooping

缺省情况下，设备的 IGMP Snooping 特性处于关闭状态。

1.5 使能IGMP Snooping

1.5.1 使能全局IGMP Snooping

1. 功能简介

使能全局 IGMP Snooping 后，设备上所有 VLAN 的 IGMP Snooping 都将使能。如果某个 VLAN 内不需要使用 IGMP Snooping，可以在该 VLAN 内关闭 IGMP snooping。

2. 配置限制和指导

使能全局 IGMP Snooping 后，若还需在某指定 VLAN 内配置其他 IGMP Snooping 功能，则必须在这些 VLAN 下使能 IGMP Snooping，否则配置的其他 IGMP Snooping 功能不生效。

使能或关闭 VLAN 内的 IGMP Snooping 的优先级高于使能全局 IGMP Snooping。例如：使能全局 IGMP Snooping 后，再在某 VLAN 视图下通过 **igmp-snooping disable** 命令关闭当前 VLAN 的 IGMP Snooping，则该 VLAN 内的 IGMP Snooping 处于关闭状态。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 IGMP-Snooping 视图。

igmp-snooping

(3) 使能全局 IGMP Snooping。

global-enable

缺省情况下，全局 IGMP Snooping 处于关闭状态。

(4) （可选）关闭某 VLAN 的 IGMP Snooping。

a. 退回系统视图。

quit

b. 进入 VLAN 视图。

vlan *vlan-id*

c. 关闭该 VLAN 的 IGMP Snooping。

igmp-snooping disable

缺省情况下，VLAN 内 IGMP Snooping 的状态与全局 IGMP Snooping 的状态保持一致。

1.5.2 使能VLAN的IGMP Snooping

1. 配置限制和指导

用户既可在 IGMP-Snooping 视图下对单个或多个 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。

在 VLAN 内使能了 IGMP Snooping 之后，IGMP Snooping 只在属于该 VLAN 的端口上生效。

2. 使能单个或多个VLAN的IGMP Snooping

(1) 进入系统视图。

system-view

(2) 进入 IGMP-Snooping 视图。

igmp-snooping

(3) 使能单个或多个 VLAN 的 IGMP Snooping。

enable vlan *vlan-list*

缺省情况下，VLAN 内 IGMP Snooping 的状态与全局 IGMP Snooping 的状态保持一致。

3. 使能单个VLAN的IGMP Snooping

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 使能该 VLAN 的 IGMP Snooping。

igmp-snooping enable

缺省情况下，VLAN 内 IGMP Snooping 的状态与全局 IGMP Snooping 的状态保持一致。

1.6 配置IGMP Snooping基本功能

1.6.1 配置IGMP Snooping版本

1. 功能简介

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 的报文以及 IGMPv3 的查询报文进行处理，对 IGMPv3 的成员关系报文则不进行处理，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。

2. 配置限制和指导

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“1.7.2 配置静态成员端口”

3. 配置多个VLAN内的IGMP Snooping版本

(1) 进入系统视图。

system-view

(2) 进入 IGMP-Snooping 视图。

igmp-snooping

(3) 配置多个 VLAN 内的 IGMP Snooping 的版本。

version *version-number* **vlan** *vlan-list*

缺省情况下，VLAN 内 IGMP Snooping 的版本为 2。

4. 配置单个VLAN内的IGMP Snooping版本

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 配置单个 VLAN 内的 IGMP Snooping 版本。

igmp-snooping version *version-number*

缺省情况下，VLAN 内 IGMP Snooping 的版本为 2。

1.6.2 配置IGMP Snooping转发表项的全局最大数量

1. 功能简介

用户可以调整 IGMP Snooping 转发表项（包括动态表项和静态表项）的全局最大数量，当设备上维护的表项数量达到或超过最大数量后，系统不再创建新的表项，也不会主动删除多余表项，直至有表项被老化或被手工删除，所以当设备上维护的表项数量达到或超过最大数量后，为避免此后无法再创建新的表项，建议用户手工删除多余表项。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 IGMP-Snooping 视图。

igmp-snooping

(3) 配置 IGMP Snooping 转发表项的全局最大数量。

entry-limit *limit*

缺省情况下，IGMP Snooping 转发表项的全局最大数量为 4294967295。

1.6.3 配置静态组播MAC地址表项

1. 功能简介

在二层组播中，除了可通过二层组播协议（如 IGMP Snooping）动态建立组播 MAC 地址表项外，还可通过手工方式配置组播 MAC 地址表项，将端口与组播 MAC 地址进行静态绑定，以便灵活控制组播信息送达的目的端口。

2. 配置限制和指导

可手工配置的组播 MAC 地址表项必须是尚未使用的组播 MAC 地址（即最高字节的最低比特位为 1 的 MAC 地址）

3. 系统视图下配置静态组播MAC地址表项

(1) 进入系统视图。

system-view

(2) 配置静态组播 MAC 地址表项。

mac-address multicast *mac-address* **interface** *interface-list* **vlan** *vlan-id*

4. 接口视图下配置静态组播MAC地址表项

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 配置静态组播 MAC 地址表项。

mac-address multicast *mac-address* **vlan** *vlan-id*

1.6.4 配置IGMP特定组查询报文的发送间隔

1. 功能简介

合理配置 IGMP 特定组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。

二层设备所发送的 IGMP 特定组查询报文，其报文的最大响应时间字段由所配置的 IGMP 特定组查询报文的发送间隔来填充，在主机在收到 IGMP 特定组查询报文后，会为其所加入的该组播组启动一个定时器，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 特定组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。

2. 全局配置IGMP特定组查询报文的发送间隔

(1) 进入系统视图。

system-view

(2) 进入 IGMP-Snooping 视图。

igmp-snooping

(3) 全局配置 IGMP 特定组查询报文的发送间隔。

last-member-query-interval *interval*

缺省情况下，IGMP 特定组查询报文的发送间隔为 1 秒。

3. 在VLAN内配置IGMP特定组查询报文的发送间隔

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 在 VLAN 内配置 IGMP 特定组查询报文的发送间隔。

igmp-snooping last-member-query-interval *interval*

缺省情况下，IGMP 特定组查询报文的发送间隔为 1 秒。

1.7 配置IGMP Snooping端口功能

1.7.1 配置动态端口老化定时器

1. 功能简介

对于动态路由器端口，如果在其老化时间内没有收到 IGMP 普遍组查询报文或者 PIM Hello 报文，二层设备将把该端口从动态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组播组的 IGMP 成员关系报告报文，二层设备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。

2. 配置限制和指导

请根据网络环境合理设置动态端口的老化时间，比如网络中组播组成员变动比较频繁，可以把动态成员端口老化时间设置小一些，避免一些无效表项老化时间过长。

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

如果二层设备向动态成员端口主动发送IGMP特定组查询报文，则该端口的老化时间将根据该IGMP特定组查询报文进行调整，调整的老化时间为 2×IGMP特定组查询报文的发送间隔。二层设备IGMP特定组查询报文发送间隔的配置，请参见“1.6.4 配置IGMP特定组查询报文的发送间隔”。

3. 全局配置动态端口老化定时器

(1) 进入系统视图。

system-view

(2) 进入 IGMP-Snooping 视图。

igmp-snooping

(3) 全局配置动态路由器端口老化时间。

router-aging-time *seconds*

缺省情况下，动态路由器端口的老化时间为 260 秒。

(4) 全局配置动态成员端口老化时间。

host-aging-time *seconds*

缺省情况下，动态成员端口的老化时间为 260 秒。

4. 在VLAN内配置动态端口老化定时器

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 在 VLAN 内配置动态路由器端口老化时间。

igmp-snooping router-aging-time *seconds*

缺省情况下，动态路由器端口的老化时间为 260 秒。

(4) 在 VLAN 内配置动态成员端口老化时间。

igmp-snooping host-aging-time *seconds*

缺省情况下，动态成员端口的老化时间为 260 秒。

1.7.2 配置静态成员端口

1. 功能简介

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。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。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 配置静态成员端口。

igmp-snooping static-group *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

缺省情况下，端口不是静态成员端口。

1.7.3 配置静态路由器端口

1. 功能简介

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

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 配置静态路由器端口。

igmp-snooping static-router-port vlan *vlan-id*

缺省情况下，端口不是静态路由器端口。

1.7.4 配置模拟主机加入

1. 功能简介

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组播组成员主机，对IGMP 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 IGMP 成员关系报告报文。
- 在模拟主机的运行过程中，当收到 IGMP 查询报文时，该端口会响应一个 IGMP 成员关系报告报文。
- 停止模拟主机时，该端口会发送一个 IGMP 离开组报文。

在二层设备的端口上配置了模拟主机加入后，模拟主机所采用的 IGMP 版本与 IGMP Snooping 的版本一致，并且该端口将作为动态成员端口参与动态成员端口的老化过程。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 配置模拟主机加入。

igmp-snooping host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

缺省情况下，未配置模拟主机加入组。

1.7.5 配置端口快速离开功能

1. 功能简介

端口快速离开是指当端口收到主机发来的离开指定组播组的 IGMP 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，二层设备不会向该端口发送或转发针对该组播组的 IGMP 特定组查询报文。

2. 配置限制和指导

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，从而导致属于同一组播组的其它接收者无法收到组播数据。

3. 全局配置端口快速离开功能

(1) 进入系统视图。

system-view

(2) 进入 IGMP-Snooping 视图。

igmp-snooping

(3) 全局开启端口快速离开功能。

fast-leave [**vlan** *vlan-list*]

缺省情况下，端口快速离开功能处于关闭状态。

4. 在端口上配置端口快速离开功能

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 在端口上开启端口快速离开功能。

igmp-snooping fast-leave [**vlan** *vlan-list*]

缺省情况下，端口快速离开功能处于关闭状态。

1.7.6 禁止端口成为动态路由器端口

1. 功能简介

在组播用户接入网络中，用户主机在某些情况下（比如测试）也会发出 IGMP 普遍组查询报文或 PIM Hello 报文：

- 如果二层设备收到了某用户主机发来的 IGMP 普遍组查询报文或 PIM Hello 报文，那么接收报文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，导致该主机收到大量无用的组播报文。
- 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。

当禁止一个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。

2. 配置限制和指导

禁止端口成为动态路由器端口的配置与静态路由器端口的配置互不影响。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 禁止端口成为动态路由器端口。

igmp-snooping router-port-deny [**vlan** *vlan-list*]

缺省情况下，端口可以成为动态路由器端口。

1.8 配置IGMP Snooping查询器

1.8.1 开启IGMP Snooping查询器

1. 功能简介

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，可以在二层设备上开启 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。

2. 配置限制和指导

请避免在运行了 IGMP 的网络中配置 IGMP Snooping 查询器，因为尽管 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。

3. 在VLAN内开启IGMP Snooping查询器

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 开启 IGMP Snooping 查询器。

igmp-snooping querier

缺省情况下，IGMP Snooping 查询器处于关闭状态。

1.8.2 开启IGMP Snooping查询器选举功能

1. 功能简介

为了避免某 VLAN 因单一 IGMP Snooping 查询器发生故障引起组播业务中断，建议在 VLAN 内配置多个 IGMP Snooping 查询器，各设备上开启 IGMP Snooping 查询器选举功能。当选举出的 IGMP Snooping 查询器发生故障无法正常工作后，VLAN 内各设备会重新选举出新的 IGMP Snooping 查询器以保证组播业务正常转发。IGMP snooping 查询器选举机制和 IGMP 查询器选举机制一样。

2. 配置准备

在VLAN内开启IGMP Snooping查询器选举功能之前，需要先开启IGMP Snooping查询器。有关开启IGMP Snooping查询器的详细介绍，请参见“1.8.1 开启IGMP Snooping查询器”

由于 IGMP Snooping 查询器收到源 IP 地址为 0.0.0.0 的查询报文和源 IP 地址与本机查询器 IP 地址相同的查询报文不进行选举，因此，用户需要通过 **igmp-snooping general-query source-ip** 命令将 IGMP 查询报文的源 IP 地址配置为一个非全零以及未被其他设备和主机使用的 IP 地址以避免上述问题。

通过 **igmp-snooping version** 命令保证参与 IGMP Snooping 查询器选举的各设备 IGMP Snooping 版本相同。

3. 在VLAN内开启IGMP Snooping查询器选举功能

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 开启 IGMP Snooping 查询器选举功能。

igmp-snooping querier-election

缺省情况下，VLAN 内 IGMP Snooping 查询器选举功能处于关闭状态。

1.8.3 配置IGMP普遍组查询和响应

1. 功能简介

可以根据网络的实际情况来修改 IGMP 普遍组查询报文的发送间隔。

合理配置 IGMP 普遍组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，其报文最大响应时间字段由所配置的 IGMP 普遍组查询的最大响应时间来填充，在主机收到 IGMP 普遍组查询报文后，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 普遍组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。

2. 配置限制和指导

为避免误删组播组成员，请确保 IGMP 普遍组查询报文的发送间隔大于 IGMP 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。

3. 全局配置IGMP普遍组查询和响应

(1) 进入系统视图。

system-view

(2) 进入 IGMP-Snooping 视图。

igmp-snooping

(3) 全局配置 IGMP 普遍组查询的最大响应时间。

max-response-time *seconds*

缺省情况下，IGMP 普遍组查询的最大响应时间为 10 秒。

4. 在VLAN内配置IGMP普遍组查询和响应

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 在 VLAN 内配置 IGMP 普遍组查询报文的发送间隔。

igmp-snooping query-interval *interval*

缺省情况下，IGMP 普遍组查询报文的发送间隔为 125 秒。

(4) 在 VLAN 内配置 IGMP 普遍组查询的最大响应时间。

igmp-snooping max-response-time *seconds*

缺省情况下，IGMP 普遍组查询的最大响应时间为 10 秒。

1.9 配置IGMP Snooping Proxy

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 在 VLAN 内开启 IGMP Snooping Proxy 功能。

igmp-snooping proxy enable

缺省情况下，VLAN 内的 IGMP Snooping Proxy 功能处于关闭状态。

1.10 调整IGMP报文

1.10.1 配置IGMP报文的源IP地址

1. 功能简介

由于 IGMP Snooping 查询器有可能发出源 IP 地址为 0.0.0.0 的查询报文，而收到此类查询报文的端口将不会被维护为动态路由器端口，从而影响动态 IGMP Snooping 转发表项的建立，最终导致组播数据无法正常转发。因此，用户可在 IGMP Snooping 查询器上通过本配置将 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。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。

用户也可以改变模拟主机或 IGMP Snooping 代理发送的 IGMP 成员关系报告报文或 IGMP 离开组报文的源 IP 地址。

2. 在VLAN内配置IGMP报文的源IP地址

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 配置 IGMP 普遍组查询报文的源 IP 地址。

igmp-snooping general-query source-ip *ip-address*

缺省情况下，IGMP 普遍组查询报文的源 IP 地址为当前 VLAN 接口的 IP 地址；若当前 VLAN 接口没有 IP 地址，则采用 0.0.0.0。

(4) 配置 IGMP 特定组查询报文的源 IP 地址。

igmp-snooping special-query source-ip *ip-address*

缺省情况下，以收到过 IGMP 普遍组查询报文的源 IP 地址作为 IGMP 特定组查询报文的源 IP 地址；否则，采用 VLAN 绑定的 VLAN 接口的 IP 地址；若该 VLAN 接口没有 IP 地址，则采用 0.0.0.0。

(5) 配置 IGMP 成员关系报告报文的源 IP 地址。

igmp-snooping report source-ip *ip-address*

缺省情况下，IGMP 成员关系报告报文的源 IP 地址为当前 VLAN 接口的 IP 地址；若当前 VLAN 接口没有 IP 地址，则采用 0.0.0.0。

(6) 配置 IGMP 离开组报文的源 IP 地址。

igmp-snooping leave source-ip *ip-address*

缺省情况下，IGMP 离开组报文的源 IP 地址为当前 VLAN 接口的 IP 地址；若当前 VLAN 接口没有 IP 地址，则采用 0.0.0.0。

1.10.2 配置IGMP报文的 802.1p优先级

1. 功能简介

当二层设备的出端口发生拥塞时，二层设备通过识别报文的 802.1p 优先级，优先发送优先级较高的报文。用户可以通过本配置改变 IGMP 报文（包括本设备生成的以及途经本设备的）的 802.1p 优先级。

2. 全局配置IGMP报文的 802.1p优先级

(1) 进入系统视图。

system-view

(2) 进入 IGMP-Snooping 视图。

igmp-snooping

(3) 全局配置 IGMP 报文的 802.1p 优先级。

dot1p-priority *priority*

缺省情况下，IGMP 报文的 802.1p 优先级为 6。

3. 在VLAN内配置IGMP报文的 802.1p优先级

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 在 VLAN 内配置 IGMP 报文的 802.1p 优先级。

igmp-snooping dot1p-priority *priority*

缺省情况下，VLAN 内 IGMP 报文的 802.1p 优先级为 6。

1.11 配置IGMP Snooping策略

1.11.1 配置组播组过滤器

1. 功能简介

在使能了 IGMP Snooping 的二层设备上，通过配置组播组过滤器，可以限制用户对组播节目的点播。本配置只对动态组播组有效，对静态组播组无效。

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，该报文将在二层设备上接受组播组过滤器的检查，只有通过了检查，二层设备才会将该主机所属的端口加入到出端口列表中，从而达到控制用户点播组播节目的目的。

2. 全局配置组播组过滤器

(1) 进入系统视图。

system-view

(2) 进入 IGMP-Snooping 视图。

igmp-snooping

(3) 全局配置组播组过滤器。

group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

缺省情况下，未配置组播组过滤器，即主机可以加入任意合法的组播组。

3. 在端口上配置组播组过滤器

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 在端口上配置组播组过滤器。

igmp-snooping group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

缺省情况下，未配置组播组过滤器，即主机可以加入任意合法的组播组。

1.11.2 配置组播数据报文源端口过滤

1. 功能简介

通过配置组播数据报文源端口过滤功能，可以允许或禁止端口作为组播源端口：

- 开启该功能后，端口不能连接组播源，因为该端口将过滤掉所有的组播数据报文（但允许组播协议报文通过），因此只能连接组播数据接收者。
- 关闭该功能后，端口既能连接组播源，也能连接组播数据接收者。

2. 配置限制和指导

在开启 IPv4 组播数据报文源端口过滤功能时，系统将同时开启 IPv6 组播数据报文源端口过滤功能。

配置组播数据报文源端口过滤在全局配置或在端口上配置的优先级相同，最新配置生效。

3. 全局配置组播数据报文源端口过滤

(1) 进入系统视图。

system-view

(2) 进入 IGMP-Snooping 视图。

igmp-snooping

(3) 开启指定端口的组播数据报文源端口过滤功能。

source-deny port *interface-list*

缺省情况下，组播数据报文源端口过滤功能处于关闭状态。

4. 在端口上配置组播数据报文源端口过滤

(1) 进入系统视图。

system-view

(2) 进入二层以太网接口视图。

interface *interface-type interface-number*

(3) 开启当前端口的组播数据报文源端口过滤功能。

igmp-snooping source-deny

缺省情况下，组播数据报文源端口过滤功能处于关闭状态。

1.11.3 配置丢弃未知组播数据报文

1. 功能简介

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：

- 当开启了丢弃未知组播数据报文功能时，二层设备只向其路由器端口转发未知组播数据报文，不在 VLAN 内广播；如果二层设备没有路由器端口，未知组播数据报文报文会被丢弃，不再转发。
- 当关闭了丢弃未知组播数据报文功能时，二层设备将在未知组播数据报文所属的 VLAN 内广播该报文。

2. 配置限制和指导

在开启了丢弃未知 IPv4 组播数据报文功能之后，未知 IPv6 组播数据报文也将被丢弃。

在开启了丢弃未知组播数据报文的功能之后，仍会向 VLAN 内的其它路由器端口转发未知组播数据报文。

3. 在VLAN内配置丢弃未知组播数据报文

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 在 VLAN 内开启丢弃未知组播数据报文功能。

igmp-snooping drop-unknown

缺省情况下，丢弃未知组播数据报文功能处于关闭状态，即对未知组播数据报文进行广播。

1.11.4 配置IGMP成员关系报告报文抑制

1. 功能简介

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。

当开启了 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。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 IGMP-Snooping 视图。

igmp-snooping

(3) 开启 IGMP 成员关系报告报文抑制功能。

report-aggregation

缺省情况下，IGMP 成员关系报告报文抑制功能处于开启状态。

1.11.5 配置端口加入的组播组最大数量

1. 功能简介

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。本配置只对动态组播组有效，对静态组播组无效。

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，系统将自动丢弃新的 IGMP 成员关系报告报文。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 配置端口加入的组播组最大数量。

igmp-snooping group-limit *limit* [**vlan** *vlan-list*]

缺省情况下，未对端口加入的组播组最大数量进行限制。

1.11.6 配置组播组替换功能

1. 功能简介

当端口上的组播组数目达到配置端口加入的组播组最大数量时，会自动丢弃新的 IGMP 成员关系报告报文。组播组替换功能开启后，当端口收到新的 IGMP 成员关系报告报文时，会自动离开 IP 地址最小的组播组并加入新的组播组。本功能主要应用于频道切换，以实现从一个组播组切换到另一个组播组。

2. 配置限制和指导

本配置只对动态组播组有效，对静态组播组无效。

当设备上维护的 IGMP Snooping 转发表项达到配置的 IGMP Snooping 转发表项的全局最大数量并且端口新加入的组播组不在设备维护的组播组列表中时，组播组替换功能不能生效。

3. 全局配置组播组替换功能

(1) 进入系统视图。

system-view

(2) 进入 IGMP-Snooping 视图。

igmp-snooping

(3) 全局开启组播组替换功能。

overflow-replace [**vlan** *vlan-list*]

缺省情况下，组播组替换功能处于关闭状态。

4. 在端口上配置组播组替换功能

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 在端口上开启组播组替换功能。

igmp-snooping overflow-replace [**vlan** *vlan-list*]

缺省情况下，组播组替换功能处于关闭状态。

1.11.7 配置IGMP Snooping主机跟踪功能

1. 功能简介

通过开启 IGMP Snooping 主机跟踪功能，可以使二层设备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、加入组播组的运行时长和超时剩余时间等），以便于网络管理员对这些主机进行监控和管理。

2. 全局配置IGMP Snooping主机跟踪功能

(1) 进入系统视图。

system-view

(2) 进入 IGMP-Snooping 视图。

igmp-snooping

(3) 全局开启 IGMP Snooping 主机跟踪功能。

host-tracking

缺省情况下，IGMP Snooping 主机跟踪功能处于关闭状态。

3. 在VLAN内配置IGMP Snooping主机跟踪功能

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 在 VLAN 内开启 IGMP Snooping 主机跟踪功能。

igmp-snooping host-tracking

缺省情况下，IGMP Snooping 主机跟踪功能处于关闭状态。

1.11.8 配置组播用户控制策略

1. 功能简介

通过配置组播用户控制策略，设备可以对组播用户发送的 IGMP 成员关系报文和 IGMP 离开报文进行过滤，从而使设备只对策略所许可的组播组维护组播成员关系。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 User-Profile 视图。

user-profile *profile-name*

本命令的详细介绍请参见“安全配置指导”中的“User Profile”。

(3) 配置组播用户控制策略。

igmp-snooping access-policy *ipv4-acl-number*

缺省情况下，未配置组播用户控制策略，即组播用户可以加入/离开任意合法的组播组。

1.12 配置设备发送的IGMP协议报文的DSCP优先级

1. 功能简介

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。通过本配置可以指定设备发送的 IGMP 协议报文的 DSCP 优先级。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 IGMP Snooping 视图。

igmp-snooping

(3) 配置设备发送的 IGMP 协议报文的 DSCP 优先级。

dscp *dscp-value*

缺省情况下，设备发送的 IGMP 协议报文的 DSCP 优先级为 48。

1.13 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 IGMP Snooping 的信息。

表1-2 IGMP Snooping 显示和维护

操作	命令
显示IGMP Snooping的状态信息	**display igmp-snooping** [**global** | **vlan** *vlan-id*]
显示动态IGMP Snooping组播组的信息	**display igmp-snooping group** [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**interface** *interface-type interface-number* | [**verbose**] [**slot** *slot-number*]]
显示IGMP Snooping主机跟踪信息	**display igmp-snooping host-tracking vlan** *vlan-id* **group** *group-address* [**source** *source-address*] [**slot** *slot-number*]
显示动态路由器端口的信息	**display igmp-snooping router-port** [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
显示静态IGMP Snooping组播组的信息	**display igmp-snooping static-group** [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
显示静态路由器端口的信息	**display igmp-snooping static-router-port** [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
显示IGMP Snooping监听到的IGMP报文和PIM hello报文的统计信息	**display igmp-snooping statistics**
显示IPv4二层组播快速转发表信息	**display l2-multicast fast-forwarding cache** [**vlan** *vlan-id*] [*source-address* | *group-address*] * [**slot** *slot-number*]
显示二层组播的IP组播组信息	**display l2-multicast ip** [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]
显示二层组播的IP转发表信息	**display l2-multicast ip forwarding** [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]
显示二层组播的MAC组播组信息	**display l2-multicast mac** [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]
显示二层组播的MAC转发表信息	**display l2-multicast mac forwarding** [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]
显示静态组播MAC地址表信息	**display mac-address** [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]]
清除动态IGMP Snooping组播组的信息	**reset igmp-snooping group** { *group-address* [*source-address*] | **all** } [**vlan** *vlan-id*]

操作	命令
清除动态路由器端口的信息	**reset igmp-snooping router-port** { **all** | **vlan** *vlan-id*}
清除IGMP Snooping监听到的IGMP报文和PIM hello报文的统计信息	**reset igmp-snooping statistics**
清除IPv4二层组播快速转发表中的转发项	**reset l2-multicast fast-forwarding cache** [**vlan** *vlan-id*] { { *source-address* | *group-address* } * | **all** } [**slot** *slot-number*]

1.14 IGMP Snooping典型配置举例

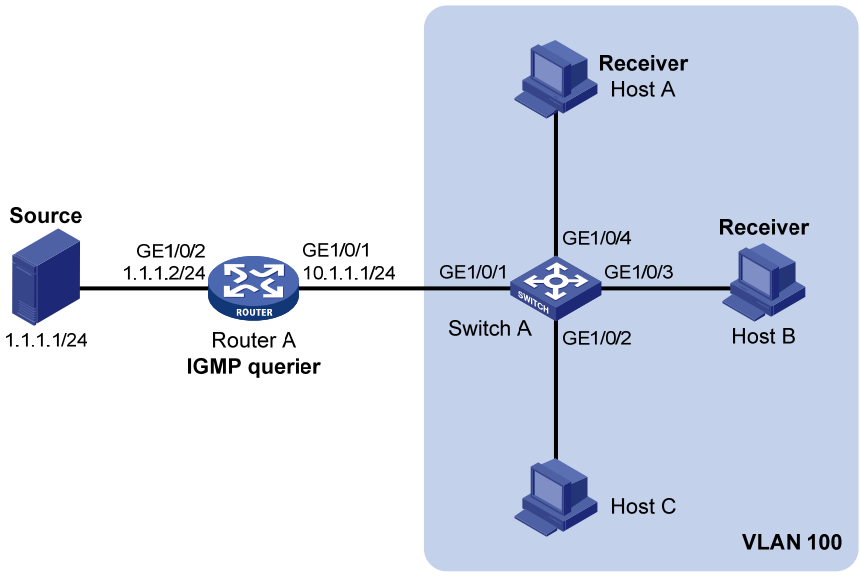
1.14.1 基于VLAN的组策略及模拟主机加入配置举例

1. 组网需求

- 如 图 1-4 所示，Router A通过GigabitEthernet1/0/2 接口连接组播源（Source），通过GigabitEthernet1/0/1 接口连接Switch A；Router A上运行IGMPv2，Switch A上运行版本 2 的IGMP Snooping，并由Router A充当IGMP查询器。
- 通过配置，使 Host A 和 Host B 能且只能接收发往组播组 224.1.1.1 的组播数据，并且当 Host A 和 Host B 发生意外而临时中断接收组播数据时，发往组播组 224.1.1.1 组播数据也能不间断地通过 Switch A 的接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 转发出去；同时，使 Switch A 将收到的未知组播数据直接丢弃，避免在其所属的 VLAN 100 内广播。

2. 组网图

图1-4 基于 VLAN 的组策略及模拟主机加入配置组网图



3. 配置步骤

(1) 配置 IP 地址

请按照 图 1-4 配置各接口的IP地址和子网掩码，具体配置过程略。

(2) 配置 Router A

使能 IP 组播路由，在接口 GigabitEthernet1/0/2 上使能 PIM-DM，并在接口 GigabitEthernet1/0/1 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

(3) 配置 Switch A

开启设备的 IGMP Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 添加到该 VLAN 中；在该 VLAN 内使能 IGMP Snooping，并开启丢弃未知组播数据报文功能。

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

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

```
[SwitchA] acl basic 2001
[SwitchA-acl-ipv4-basic-2001] rule permit source 224.1.1.1 0
[SwitchA-acl-ipv4-basic-2001] quit
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] group-policy 2001 vlan 100
[SwitchA-igmp-snooping] quit
```

在 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 上分别配置模拟主机加入组播组 224.1.1.1。

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet1/0/4] quit
```

4. 验证配置

假设组播源分别向组播组 224.1.1.1 和 224.2.2.2 发送的组播数据，Host A 和 Host B 也都申请加入这两个组播组。

显示 Switch A 上 VLAN 100 内动态 IGMP Snooping 组播组的信息。

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

```
VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (2 in total):
      GE1/0/3                                  (00:03:23)
      GE1/0/4                                  (00:04:10)
```

由此可见，Host A 和 Host B 所在的端口 GigabitEthernet1/0/4 和 GigabitEthernet1/0/3 均已加入组播组 224.1.1.1，但都未加入组播组 224.2.2.2，这表明组播组过滤器已生效。

1.14.2 基于VLAN的静态端口配置举例

1. 组网需求

- 如 图 1-5 所示，Router A通过GigabitEthernet1/0/2 接口连接组播源（Source），通过 GigabitEthernet1/0/1 接口连接Switch A；Router A上运行IGMPv2，Switch A、Switch B和 Switch C上都运行版本 2 的IGMP Snooping，并由Router A充当IGMP查询器。
- Host A 和 Host C 均为组播组 224.1.1.1 的固定接收者（Receiver），通过将 Switch C 上的端口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/5 配置为组播组 224.1.1.1 的静态成员端口，可以增强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，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 GigabitEthernet1/0/3 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，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。

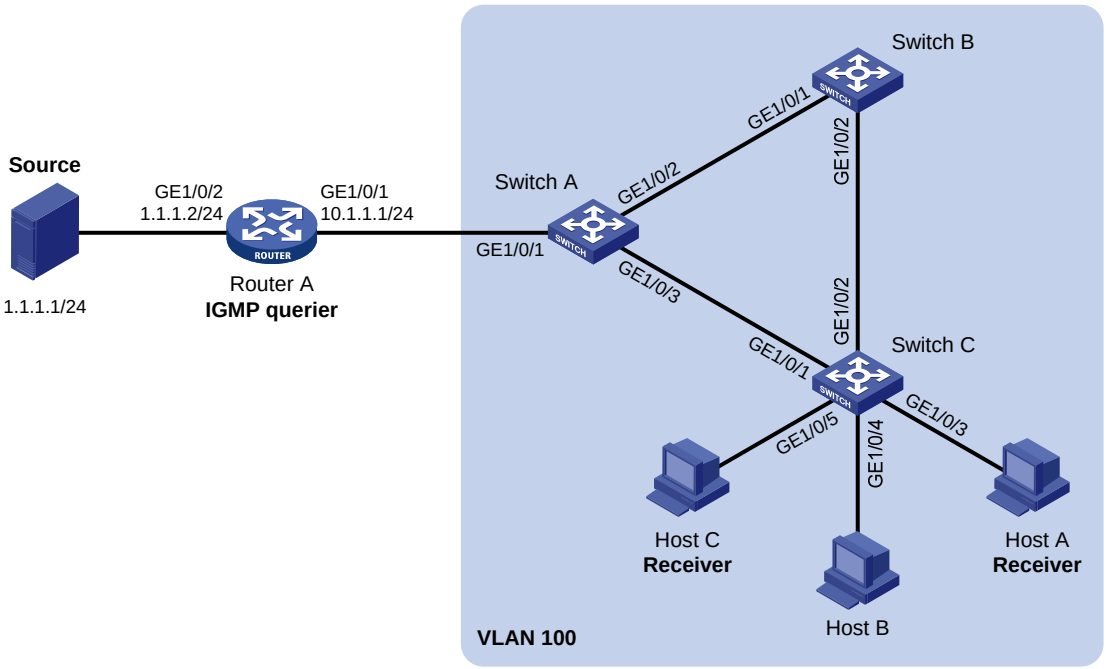
说明

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 IGMP 查询和响应周期完成后，组播数据才能通过 Switch A—Switch C 的新路径传递给接收者，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1-5 基于 VLAN 的静态端口配置组网图



3. 配置步骤

(1) 配置 IP 地址

请按照 图 1-5 配置各接口的IP地址和子网掩码，具体配置过程略。

(2) 配置 Router A

使能 IP 组播路由，在接口 GigabitEthernet1/0/2 上使能 PIM-DM，并在接口 GigabitEthernet1/0/1 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

(3) 配置 Switch A

开启设备的 IGMP Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/3 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchA] vlan 100
```

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

把 GigabitEthernet1/0/3 配置为静态路由器端口。

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] igmp-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

(4) 配置 Switch B

开启设备的 IGMP Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping。

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

(5) 配置 Switch C

开启设备的 IGMP Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/5 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping。

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

分别在端口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/5 上配置静态加入组播组 224.1.1.1。

```
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-GigabitEthernet1/0/3] quit
[SwitchC] interface gigabitethernet 1/0/5
[SwitchC-GigabitEthernet1/0/5] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-GigabitEthernet1/0/5] 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 igmp-snooping static-router-port vlan 100
VLAN 100:
  Router ports (1 in total):
    GE1/0/3
```

由此可见，Switch A 上的端口 GigabitEthernet1/0/3 已经成为了静态路由器端口。

显示 Switch C 上 VLAN 100 内静态 IGMP Snooping 组播组的信息。

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

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (2 in total):
      GE1/0/3
      GE1/0/5
```

由此可见，Switch C 上的端口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/5 已经成为了组播组 224.1.1.1 的静态成员端口。

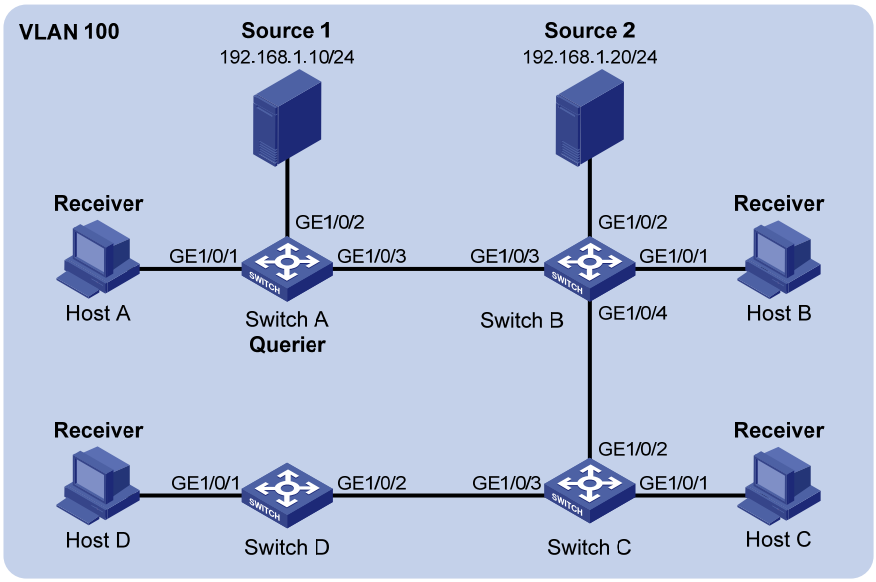
1.14.3 基于VLAN的IGMP Snooping查询器配置举例

1. 组网需求

- 如 图 1-6 所示，在一个没有三层设备的纯二层网络环境中，组播源Source 1 和Source 2 分别向组播组 224.1.1.1 和 225.1.1.1 发送组播数据，Host A和Host C是组播组 224.1.1.1 的接收者（Receiver），Host B和Host D则是组播组 225.1.1.1 的接收者；所有接收者均使用IGMPv2，所有交换机上都运行版本 2 的IGMP Snooping，并选择距组播源较近的Switch A来充当IGMP Snooping查询器。
- 为防止交换机在没有二层组播转发表项时将组播数据在 VLAN 内广播，在所有交换机上都开启丢弃未知组播数据报文功能；同时，由于交换机不会将收到源 IP 地址为 0.0.0.0 的 IGMP 查询报文的端口设置为动态路由器端口，从而会影响二层组播转发表项的建立并导致组播数据无法正常转发，因此需要将 IGMP 查询报文的源 IP 地址配置为非 0.0.0.0 以避免此问题。

2. 组网图

图1-6 基于 VLAN 的 IGMP Snooping 查询器配置组网图



3. 配置步骤

(1) 配置 Switch A

开启设备的 IGMP Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/3 添加到该 VLAN 中；在该 VLAN 内使能 IGMP Snooping，并开启丢弃未知组播数据报文功能。

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

在 VLAN 100 内开启 IGMP Snooping 查询器。

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

在 VLAN 100 内将 IGMP 普遍组查询和特定组查询报文的源 IP 地址均配置为 192.168.1.1。

```
[SwitchA-vlan100] igmp-snooping general-query source-ip 192.168.1.1
[SwitchA-vlan100] igmp-snooping special-query source-ip 192.168.1.1
[SwitchA-vlan100] quit
```

(2) 配置 Switch B

开启设备的 IGMP Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 添加到该 VLAN 中；在该 VLAN 内使能 IGMP Snooping，并开启丢弃未知组播数据报文功能。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] igmp-snooping drop-unknown
[SwitchB-vlan100] quit
```

(3) 配置 Switch C

开启设备的 IGMP Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/3 添加到该 VLAN 中；在该 VLAN 内使能 IGMP Snooping，并开启丢弃未知组播数据报文功能。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[SwitchC-vlan100] igmp-snooping enable
[SwitchC-vlan100] igmp-snooping drop-unknown
[SwitchC-vlan100] quit
```

(4) 配置 Switch D

开启设备的 IGMP Snooping 特性。

```
<SwitchD> system-view
[SwitchD] igmp-snooping
```

```
[SwitchD-igmp-snooping] quit
```

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/2 添加到该 VLAN 中；在该 VLAN 内使能 IGMP Snooping，并开启丢弃未知组播数据报文功能。

```
[SwitchD] vlan 100
[SwitchD-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[SwitchD-vlan100] igmp-snooping enable
[SwitchD-vlan100] igmp-snooping drop-unknown
[SwitchD-vlan100] quit
```

4. 验证配置

当 IGMP 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 IGMP 普遍组查询报文。

显示 Switch B 上收到的 IGMP 报文的统计信息。

```
[SwitchB] display igmp-snooping statistics
Received IGMP general queries:  3
Received IGMPv1 reports:  0
Received IGMPv2 reports:  12
Received IGMP leaves:  0
Received IGMPv2 specific queries:  0
Sent     IGMPv2 specific queries:  0
Received IGMPv3 reports:  0
Received IGMPv3 reports with right and wrong records:  0
Received IGMPv3 specific queries:  0
Received IGMPv3 specific sg queries:  0
Sent     IGMPv3 specific queries:  0
Sent     IGMPv3 specific sg queries:  0
Received PIMv2 hello:  0
Received error IGMP messages:  0
```

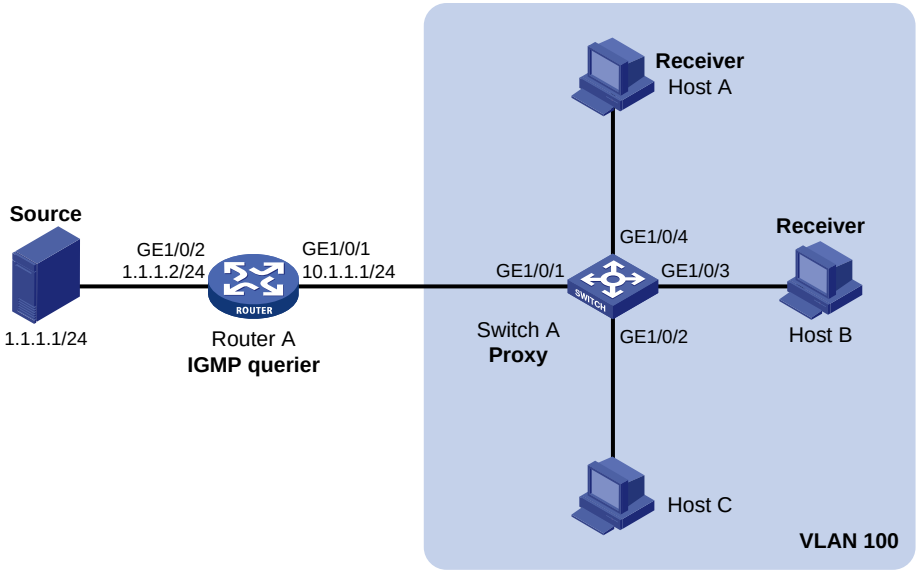
1.14.4 基于VLAN的IGMP Snooping Proxy配置举例

1. 组网需求

- 如 图 1-7 所示，Router A通过GigabitEthernet1/0/2 接口连接组播源（Source），通过GigabitEthernet1/0/1 接口连接Switch A；Router A上运行IGMPv2，Switch A上运行版本 2 的IGMP Snooping，并由Router A充当IGMP查询器。
- 通过配置，使 Switch A 能够代理下游主机向 Router A 发送的 IGMP 报告报文和离开报文，以及响应 Router A 发来的 IGMP 查询报文并向下游主机转发。

2. 组网图

图1-7 基于 VLAN 的 IGMP Snooping Proxy 配置组网图



3. 配置步骤

(1) 配置 IP 地址

请按照 图 1-7 配置各接口的IP地址和子网掩码，具体配置过程略。

(2) 配置 Router A

使能 IP 组播路由，在接口 GigabitEthernet1/0/2 上使能 PIM-DM，并在接口 GigabitEthernet1/0/1 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] pim dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

(3) 配置 Switch A

开启设备的 IGMP Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 添加到该 VLAN 中；在该 VLAN 内使能 IGMP Snooping，并使能 IGMP Snooping Proxy。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchA-vlan100] igmp-snooping enable
```

```
[SwitchA-vlan100] igmp-snooping proxy enable
[SwitchA-vlan100] quit
```

4. 验证配置

当配置完成后，Host A 和 Host B 分别发送组地址为 224.1.1.1 的 IGMP 加入报文，Switch A 收到该报文后通过其路由器端口 GigabitEthernet1/0/1 向 Router A 也发送该组的加入报文。通过使用 **display igmp-snooping group** 和 **display igmp group** 命令可以分别查看 IGMP Snooping 组和 IGMP 组的信息，例如：

查看 Switch A 上 IGMP Snooping 组播组的信息。

```
[SwitchA] display igmp-snooping group
 Total 1 entries.

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (2 in total):
      GE1/0/3                                  (00:04:00)
      GE1/0/4                                  (00:04:04)
```

查看 Router A 上 IGMP 组的信息。

```
[RouterA] display igmp group
IGMP groups in total: 1
 GigabitEthernet1/0/1(10.1.1.1):
  IGMP groups reported in total: 1
   Group address   Last reporter   Uptime      Expires
   224.1.1.1       0.0.0.0         00:00:31    00:02:03
```

当 Host A 离开组播组 224.1.1.1 时，向 Switch A 发送该组的 IGMP 离开报文，但由于 Host B 仍未离开该组，因此 Switch A 并不会删除该组，也不会向 Router A 发送该组的离开报文，只是在该组对应转发表项的成员端口列表中将端口 GigabitEthernet1/0/4 删除。通过使用 **display igmp-snooping group** 命令可以查看 IGMP Snooping 组的信息，例如：

查看 Switch A 上 IGMP Snooping 组播组的信息。

```
[SwitchA] display igmp-snooping group
Total 1 entries.

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (1 in total):
      GE1/0/3                                  ( 00:01:23 )
```

1.15 IGMP Snooping常见故障处理

1.15.1 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 IGMP Snooping 二层组播功能。

2. 故障分析

IGMP Snooping 没有使能。

3. 处理过程

(1) 使用 **display igmp-snooping** 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** 命令开启设备的 IGMP Snooping 特性，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。

1.15.2 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. 故障分析

- ACL 规则配置不正确；
- 组播组策略应用不正确；
- 没有开启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 igmp-snooping** 命令查看是否已开启丢弃未知组播数据报文的功能。如果没有开启，则使用 **igmp-snooping drop-unknown** 命令开启丢弃未知组播数据报文功能。

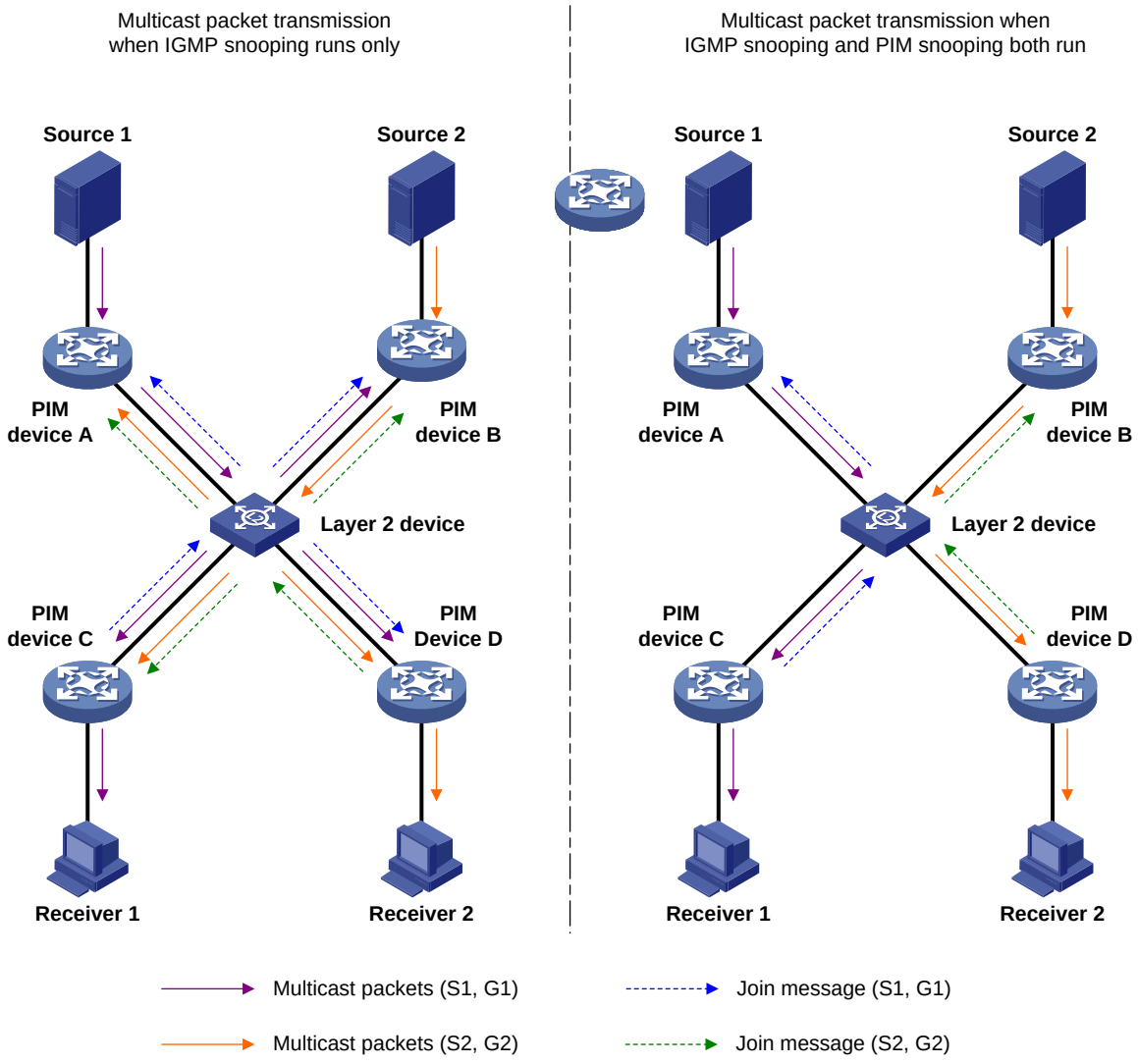
目 录

1 PIM Snooping

1.1 PIM Snooping简介

PIM Snooping（Protocol Independent Multicast Snooping，协议无关组播窥探）运行在二层设备上，通过与 IGMP Snooping 配合来对收到的 PIM 协议报文进行分析，将有接收需求的端口添加到 PIM Snooping 路由表的相应表项中，以实现组播报文的精确转发。

图1-1 二层设备运行 PIM Snooping 前后的对比



如 图 1-1 所示，组播源Source 1 和Source 2 分别向组播组G1 和G2 发送组播数据，而Receiver 1 和Receiver 2 则分别是G1 和G2 的接收者，二层设备上连接各PIM路由器的端口都属于同一个VLAN：

- 当二层设备只运行 IGMP Snooping 时，它通过监听 PIM 路由器发出的 PIM Hello 报文来维护路由器端口，将组播数据报文向 VLAN 内的所有路由器端口转发，而将除 PIM Hello 报文外的

其它 PIM 协议报文在 VLAN 内广播。因此，无论 PIM 路由器是否有接收需求，都会收到所有的 PIM 协议报文和组播数据报文。

- 当二层设备同时运行了 IGMP Snooping 和 PIM Snooping 时，它通过监听 PIM 路由器发出的 PIM 协议报文来了解其接收需求，将有接收需求的 PIM 路由器所在的端口添加到 PIM Snooping 路由表的相应表项中，使 PIM 协议报文和组播数据报文能够被精确转发给有接收需求的 PIM 路由器，从而节约了网络带宽。

说明

有关 IGMP Snooping 和路由器端口的详细介绍，请参见“IP 组播配置指导”中的“IGMP Snooping”。

1.2 PIM Snooping配置限制和指导

PIM Snooping 功能在 Secondary VLAN 中不会生效，因此不建议在 Secondary VLAN 中配置此功能。有关 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“Private VLAN”。

在 VLAN 内使能了 PIM Snooping 之后，PIM Snooping 功能只在属于该 VLAN 的端口上生效。

1.3 PIM Snooping配置任务简介

PIM Snooping 配置任务如下：

(1) 使能PIM Snooping

(2) （可选）配置主从倒换后PIM Snooping全局端口的老化时间

- 配置全局邻居端口的老化时间
- 配置全局下游端口和全局路由器端口的老化时间

1.4 使能PIM Snooping

(1) 进入系统视图。

system-view

(2) 开启设备的 IGMP Snooping，并进入 IGMP-Snooping 视图。

igmp-snooping

缺省情况下，IGMP Snooping 处于关闭状态。

本命令的详细介绍，请参见“IP 组播命令参考”中的“IGMP Snooping”。

(3) 退回系统视图。

quit

(4) 进入 VLAN 视图。

vlan *vlan-id*

(5) VLAN 内使能 IGMP Snooping。

igmp-snooping enable

缺省情况下，VLAN 内的 IGMP Snooping 处于关闭状态。

本命令的详细介绍，请参见“IP 组播命令参考”中的“IGMP Snooping”。

(6) VLAN 内使能 PIM Snooping。

pim-snooping enable

缺省情况下，VLAN 内的 PIM Snooping 处于关闭状态。

1.5 配置主从倒换后PIM Snooping全局端口的老化时间

1.5.1 功能简介

全局端口指的是主设备的虚拟端口，包括二层聚合接口等。由全局端口担任的邻居端口、下游端口和路由器端口分别称为全局邻居端口、全局下游端口和全局路由器端口。

为了使 PIM Snooping 在主从倒换后不会因表项老化而影响二层数据转发，可以手动配置倒换后的全局端口老化时间。

1.5.2 配置限制和指导

当主从倒换后的全局邻居端口收到 PIM Hello 报文时，手动配置的全局邻居端口的老化时间将失效，以 PIM Hello 报文里的老化时间为准。

当主从倒换后的全局路由器端口和全局下游端口收到 PIM 加入报文时，手动配置的全局路由器端口和全局下游端口的老化时间将失效，以 PIM 加入报文里的老化时间为准。

1.5.1 配置全局邻居端口的老化时间

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 配置主从倒换后 PIM Snooping 全局邻居端口的老化时间。

pim-snooping graceful-restart neighbor-aging-time *seconds*

缺省情况下，主从倒换后 PIM Snooping 全局邻居端口老化时间为 105 秒。

1.5.2 配置全局下游端口和全局路由器端口的老化时间

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 配置主从倒换后 PIM Snooping 全局下游端口和全局路由器端口的老化时间。

pim-snooping graceful-restart join-aging-time *seconds*

缺省情况下，主从倒换后 PIM Snooping 全局下游端口和全局路由器端口的老化时间为 210 秒。

1.6 PIM 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 PIM 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 PIM Snooping 的统计信息。

表1-1 PIM Snooping 显示和维护

操作	命令
显示PIM Snooping的邻居信息	**display pim-snooping neighbor** [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]
显示PIM Snooping的路由器端口信息	**display pim-snooping router-port** [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]
显示PIM Snooping路由表的信息	**display pim-snooping routing-table** [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]
显示PIM Snooping监听到的PIM报文的统计信息	**display pim-snooping statistics**
清除PIM Snooping监听到的PIM报文的统计信息	**reset pim-snooping statistics**

1.7 PIM Snooping典型配置举例

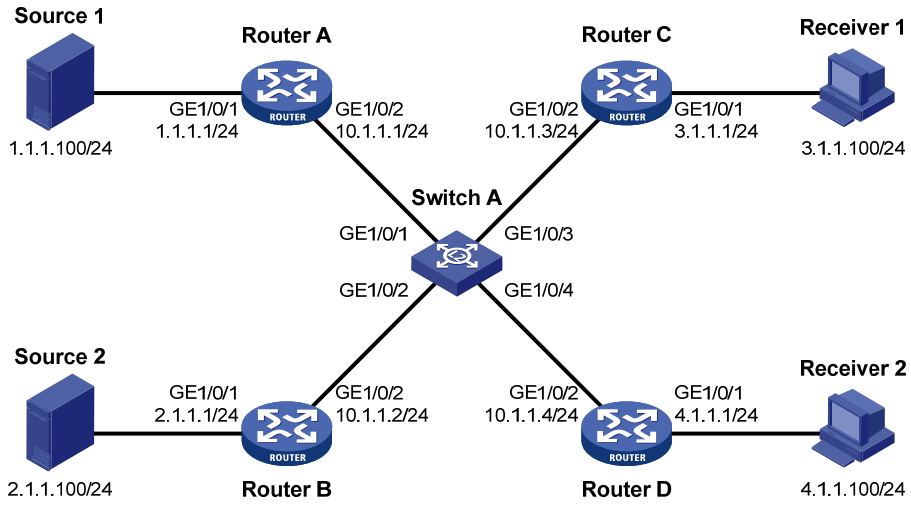
1.7.1 PIM Snooping基本组网配置举例

1. 组网需求

- 如 图 1-2 所示，网络中运行OSPF协议，Router A和Router B各自的GigabitEthernet1/0/1 接口分别连接组播源Source 1 和Source 2；Router C和Router D各自的GigabitEthernet1/0/1 接口分别连接接收者Receiver 1 和Receiver 2；Router A、Router B、Router C和Router D各自的GigabitEthernet1/0/2 接口都通过Switch A互连。
- Source 1 和 Source 2 分别通过组播组 224.1.1.1 和 225.1.1.1 发送组播数据，Receiver 1 和 Receiver 2 则分别接收来自组播组 224.1.1.1 和 225.1.1.1 的组播数据；Router C 和 Router D 各自的 GigabitEthernet1/0/1 接口上都运行 IGMP，Router A、Router B、Router C 和 Router D 上都运行 PIM-SM，并由 Router A 的 GigabitEthernet1/0/2 接口充当 C-BSR 和 C-RP。
- 通过在 Switch A 上配置 IGMP Snooping 和 PIM Snooping，使 Switch A 将 PIM 协议报文和组播数据报文只转发给有接收需求的路由器。
- 在所有与 Switch A 相连的 PIM 设备上配置加入/剪枝报文的最大长度为 1400 字节，小于路径 MTU。

2. 组网图

图1-2 PIM Snooping 典型配置组网图



3. 配置步骤

(1) 配置 IP 地址和单播路由协议

请按照 图 1-2 配置各接口的IP地址和子网掩码，并在各路由器上配置OSPF协议，具体配置过程略。

(2) 配置 Router A

使能 IP 组播路由，在各接口上使能 PIM-SM，设置加入/剪枝报文的最大长度，并配置 C-BSR 和 C-RP。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pim sm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim sm
[RouterA-GigabitEthernet1/0/2] quit
[RouterA] pim
[RouterA-pim] jp-pkt-size 1400
[RouterA-pim] c-bsr 10.1.1.1
[RouterA-pim] c-rp 10.1.1.1
[RouterA-pim] quit
```

(3) 配置 Router B

使能 IP 组播路由，在各接口上使能 PIM-SM，并设置加入/剪枝报文的最大长度。

```
<RouterB> system-view
[RouterB] multicast routing
[RouterB-mrib] quit
[RouterB] interface gigabitethernet 1/0/1
```

```
[RouterB-GigabitEthernet1/0/1] pim sm
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] pim sm
[RouterB-GigabitEthernet1/0/2] quit
[RouterB] pim
[RouterB-pim] jp-pkt-size 1400
```

(4) 配置 Router C

使能 IP 组播路由，在接口 GigabitEthernet1/0/2 上使能 PIM-SM，在接口 GigabitEthernet1/0/1 上使能 IGMP，并设置加入/剪枝报文的最大长度。

```
<RouterC> system-view
[RouterC] multicast routing
[RouterC-mrib] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] igmp enable
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] pim sm
[RouterC-GigabitEthernet1/0/2] quit
[RouterC] pim
[RouterC-pim] jp-pkt-size 1400
```

(5) 配置 Router D

使能 IP 组播路由，在接口 GigabitEthernet1/0/2 上使能 PIM-SM，并在接口 GigabitEthernet1/0/1 上使能 IGMP，并设置加入/剪枝报文的最大长度。

```
<RouterD> system-view
[RouterD] multicast routing
[RouterD-mrib] quit
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] igmp enable
[RouterD-GigabitEthernet1/0/1] quit
[RouterD] interface gigabitethernet 1/0/2
[RouterD-GigabitEthernet1/0/2] pim sm
[RouterD-GigabitEthernet1/0/2] quit
[RouterD] pim
[RouterD-pim] jp-pkt-size 1400
```

(6) 配置 Switch A

开启设备的 IGMP Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping 和 PIM Snooping。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] pim-snooping enable
```

```
    [SwitchA-vlan100] quit
```

4. 验证配置

显示 Switch A 上 VLAN 100 内 PIM Snooping 的邻居信息。

```
[SwitchA] display pim-snooping neighbor vlan 100
Total 4 neighbors.

VLAN 100: Total 4 neighbors.
  10.1.1.1
    Ports (1 in total):
      GE1/0/1                 (00:32:43)
  10.1.1.2
    Ports (1 in total):
      GE1/0/2                 (00:32:43)
  10.1.1.3
    Ports (1 in total):
      GE1/0/3                 (00:32:43)
  10.1.1.4
    Ports (1 in total):
      GE1/0/4                 (00:32:43)
```

由此可见，Router A、Router B、Router C 和 Router D 之间都建立起了 PIM Snooping 邻居关系。

显示 Switch A 上 VLAN 100 内 PIM Snooping 路由表的信息。

```
[SwitchA] display pim-snooping routing-table vlan 100
Total 2 entries.
FSM Flag: NI-no info, J-join, PP-prune pending

VLAN 100: Total 2 entries.
  (*, 224.1.1.1)
    Upstream neighbor: 10.1.1.1
      Upstream Ports (1 in total):
        GE1/0/1
      Downstream Ports (1 in total):
        GE1/0/3
          Expires: 00:03:01, FSM: J
  (*, 225.1.1.1)
    Upstream neighbor: 10.1.1.2
      Upstream Ports (1 in total):
        GE1/0/2
      Downstream Ports (1 in total):
        GE1/0/4
          Expires: 00:03:11, FSM: J
```

由此可见，Switch A 将向 Router C 转发组播组 224.1.1.1 的组播数据，向 Router D 转发组播组 225.1.1.1 的组播数据。

1.8 PIM Snooping常见故障处理

1.8.1 二层设备不能实现PIM Snooping功能

1. 故障现象

二层设备不能实现 PIM Snooping 功能。

2. 故障分析

IGMP Snooping 或 PIM Snooping 没有使能。

3. 处理过程

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

(2) 如果没有使能 IGMP Snooping，请先开启设备的 IGMP Snooping，然后分别使能 VLAN 内的 IGMP Snooping 和 PIM Snooping。

(3) 如果没有使能 PIM Snooping，请使能 VLAN 内的 PIM Snooping。

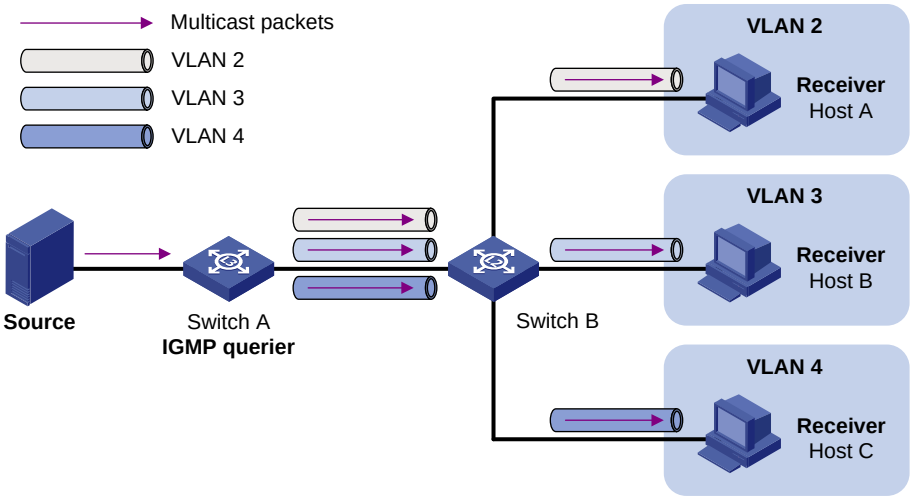
目 录

1 组播VLAN

1.1 组播VLAN作用

如 图 1-1 所示，在传统的组播点播方式下，当属于不同VLAN的主机Host A、Host B和Host C同时点播同一组播组时，三层设备（Switch A）需要将组播数据为每个用户VLAN（即主机所属的VLAN）都复制一份后发送给二层设备（Switch B）。这样既造成了带宽的浪费，也给三层设备增加了额外的负担。

图1-1 未运行组播 VLAN 时的组播数据传输



可以使用组播 VLAN 功能解决这个问题。在二层设备上配置了组播 VLAN 后，三层设备只需将组播数据通过组播 VLAN 向二层设备发送一份即可，而不必向每个用户 VLAN 都复制一份，从而节省了网络带宽，也减轻了三层设备的负担。

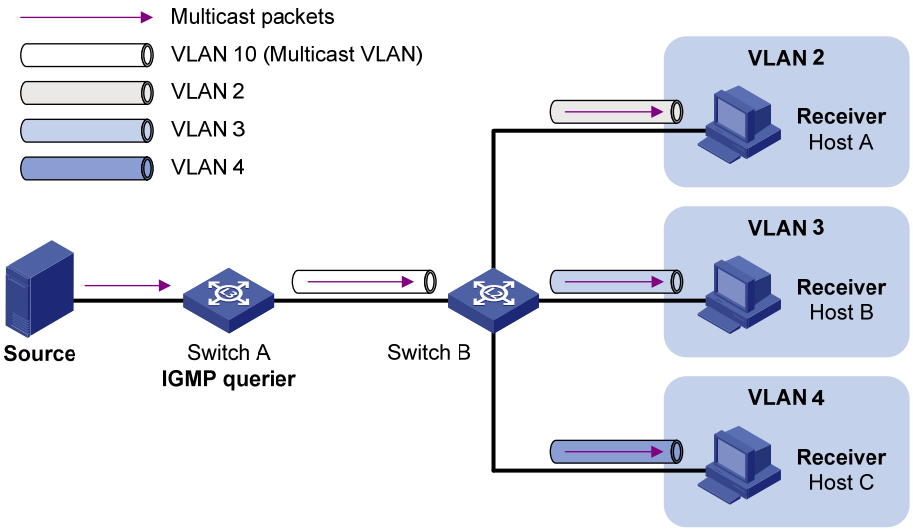
1.2 组播VLAN实现方式

组播 VLAN 有基于子 VLAN 和基于端口两种实现和配置方式。

1.2.1 基于子VLAN的组播VLAN

如 图 1-2 所示，接收者主机Host A、Host B和Host C分属不同的用户VLAN。在Switch B上配置VLAN 10为组播VLAN，将所有的用户VLAN都配置为该组播VLAN的子VLAN，并在组播VLAN及其子VLAN内都使能IGMP Snooping。

图1-2 基于子 VLAN 的组播 VLAN 示意图

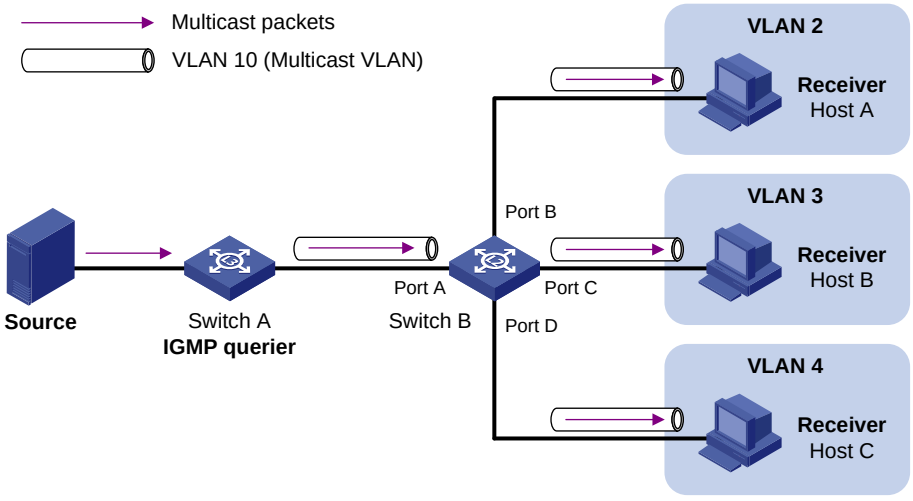


配置完成后，IGMP Snooping 将在组播 VLAN 中对路由器端口进行维护，而在各子 VLAN 中对成员端口进行维护。这样，Switch A 只需将组播数据通过组播 VLAN 向 Switch B 发送一份即可，Switch B 会将其复制分发给该组播 VLAN 内那些有接收者的子 VLAN。

1.2.2 基于端口的组播VLAN

如 图 1-3 所示，接收者主机Host A、Host B和Host C分属不同的用户VLAN，Switch B上的所有用户端口（即连接主机的端口）均为Hybrid类型。在Switch B上配置VLAN 10 为组播VLAN，将所有用户端口都添加到该组播VLAN内，并在组播VLAN和所有用户VLAN内都使能IGMP Snooping。

图1-3 基于端口的组播 VLAN 示意图



配置完成后，当 Switch B 上的用户端口收到来自主机的 IGMP 报文时，会为其打上组播 VLAN 的 Tag 并上送给 IGMP 查询器，于是 IGMP Snooping 就可以在组播 VLAN 中对路由器端口和成员端口进行统一的维护。这样，Switch A 只需将组播数据通过组播 VLAN 向 Switch B 发送一份即可，Switch B 会将其复制分发给该组播 VLAN 内的所有成员端口。

1.3 组播VLAN配置限制和指导

要配置为组播 VLAN 的指定 VLAN 必须存在。

若在设备上同时配置了基于子 VLAN 和基于端口的组播 VLAN，则基于端口的组播 VLAN 将优先生效。

组播 VLAN 功能在 Secondary VLAN 中不会生效，因此不建议在 Secondary VLAN 中配置此功能。有关 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“Private VLAN”。

1.4 配置基于子VLAN的组播VLAN

1. 配置限制和指导

要添加到组播 VLAN 内的子 VLAN 必须存在，且不能是组播 VLAN 或其它组播 VLAN 的子 VLAN。

2. 配置准备

在配置基于子 VLAN 的组播 VLAN 之前，需完成以下任务：

- 创建相应的 VLAN
- 在欲配置为组播 VLAN 及其子 VLAN 的所有 VLAN 内都使能 IGMP Snooping

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置指定 VLAN 为组播 VLAN，并进入组播 VLAN 视图。

multicast-vlan *vlan-id*

缺省情况下，VLAN 不是组播 VLAN。

(3) 向组播 VLAN 内添加子 VLAN。

subvlan *vlan-list*

1.5 配置基于端口的组播VLAN

1. 配置限制和指导

既可以在组播 VLAN 内添加端口，也可以在端口上指定其所属的组播 VLAN——这两种配置方式是等效的。

一个端口只能属于一个组播 VLAN。

2. 配置准备

在配置基于端口的组播 VLAN 之前，需完成以下任务：

- 创建相应的 VLAN
- 在欲配置为组播 VLAN 的 VLAN 内使能 IGMP Snooping
- 在所有的用户 VLAN 内都使能 IGMP Snooping
- 配置用户端口属性，保证当二层设备通过组播 VLAN 收到来自上游、打有组播 VLAN Tag 的组播数据报文时，会将其 Tag 去掉后再向下游转发。有关配置用户端口属性的详细介绍，请参见“二层技术-以太网交换命令参考”中的“VLAN”。

3. 在组播VLAN内配置组播VLAN端口

(1) 进入系统视图。

system-view

(2) 配置指定 VLAN 为组播 VLAN，并进入组播 VLAN 视图。

multicast-vlan *vlan-id*

缺省情况下，VLAN 不是组播 VLAN。

(3) 向组播 VLAN 内添加端口。

port *interface-list*

4. 在端口上配置组播VLAN端口

(1) 进入系统视图。

system-view

(2) 配置指定 VLAN 为组播 VLAN，并进入组播 VLAN 视图。

multicast-vlan *vlan-id*

缺省情况下，VLAN 不是组播 VLAN。

(3) 退回系统视图。

quit

(4) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(5) 指定端口所属的组播 VLAN。

port multicast-vlan *vlan-id*

缺省情况下，端口不属于任何组播 VLAN。

1.6 配置组播VLAN转发表项的最大数量

1. 功能简介

用户可以调整组播 VLAN 转发表项的最大数量，当所有组播 VLAN 内维护的表项总数达到最大数量后，将不再创建新的表项，直至有表项被老化或被手工删除。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置组播 VLAN 转发表项的最大数量。

multicast-vlan entry-limit *limit*

缺省情况下，组播 VLAN 转发表项的最大数量为 1000。

1.7 组播VLAN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组播 VLAN 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 VLAN 的统计信息。

表1-1 组播 VLAN 显示和维护

操作	命令
显示组播VLAN的信息	**display multicast-vlan** [*vlan-id*]
显示组播VLAN转发表的信息	**display multicast-vlan forwarding-table** [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **slot** *slot-number* | **subvlan** *vlan-id* | **vlan** *vlan-id*] *
显示组播VLAN的组播组表项信息	**display multicast-vlan group** [*source-address* | *group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *
清除组播VLAN的组播组表项	**reset multicast-vlan group** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **vlan** *vlan-id*] *

1.8 组播VLAN典型配置举例

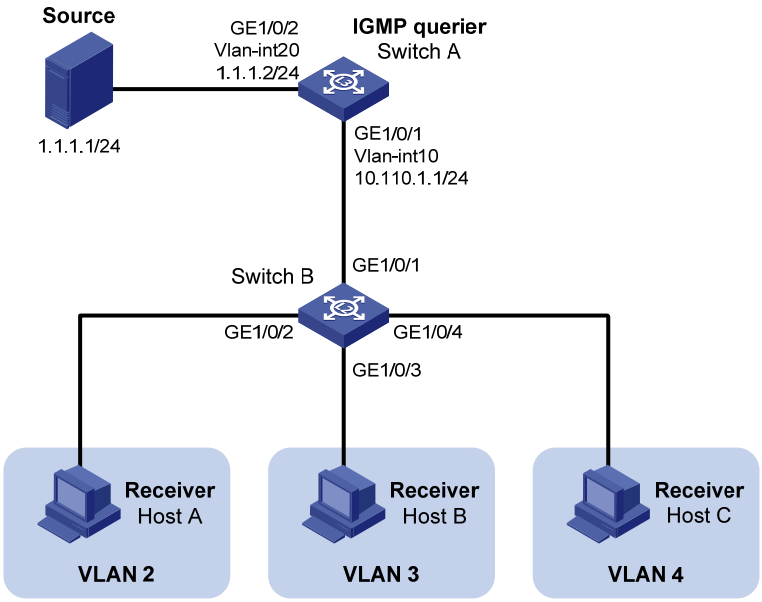
1.8.1 基于子VLAN的组播VLAN配置举例

1. 组网需求

- 如 图 1-4 所示，三层交换机Switch A通过接口VLAN-interface20 连接组播源（Source），通过接口VLAN-interface10 连接二层交换机Switch B；Switch A上运行IGMPv2，Switch B上运行版本 2 的IGMP Snooping，并由Switch A充当IGMP查询器。
- 组播源向组播组 224.1.1.1 发送组播数据，Host A～Host C 都是该组播组的接收者（Receiver），且分别属于 VLAN 2～VLAN 4。
- 通过在 Switch B 上配置基于子 VLAN 的组播 VLAN，使 Switch A 通过组播 VLAN 向 Switch B 下分属不同用户 VLAN 的主机分发组播数据。

2. 组网图

图1-4 基于子 VLAN 的组播 VLAN 配置组网图



3. 配置步骤

(1) 配置 Switch A

使能 IP 组播路由。

```
<SwitchA> system-view
[SwitchA] multicast routing
[SwitchA-mrib] quit
```

创建 VLAN 20，并将端口 GigabitEthernet1/0/2 加入该 VLAN。

```
[SwitchA] vlan 20
[SwitchA-vlan20] port gigabitethernet 1/0/2
[SwitchA-vlan20] quit
```

在接口 VLAN-interface20 上配置 IP 地址，并使能 PIM-DM。

```
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ip address 1.1.1.2 24
[SwitchA-Vlan-interface20] pim dm
[SwitchA-Vlan-interface20] quit
```

创建 VLAN 10，配置端口 GigabitEthernet1/0/1 为 Hybrid 端口，并允许 VLAN 10 的报文带 Tag 通过。

```
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type hybrid
[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 10 tagged
[SwitchA-GigabitEthernet1/0/1] quit
```

在接口 VLAN-interface10 上配置 IP 地址，并使能 IGMP。

```
[SwitchA] interface vlan-interface 10
```

```
[SwitchA-Vlan-interface10] ip address 10.110.1.1 24
[SwitchA-Vlan-interface10] igmp enable
[SwitchA-Vlan-interface10] quit
```

(2) 配置 Switch B

开启设备的 IGMP Snooping。

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

创建 VLAN 2，将端口 GigabitEthernet1/0/2 加入该 VLAN，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/2
[SwitchB-vlan2] igmp-snooping enable
[SwitchB-vlan2] quit
```

创建 VLAN 3，将端口 GigabitEthernet1/0/3 加入该 VLAN，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/3
[SwitchB-vlan3] igmp-snooping enable
[SwitchB-vlan3] quit
```

创建 VLAN 4，将端口 GigabitEthernet1/0/4 加入该 VLAN，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchB] vlan 4
[SwitchB-vlan4] port gigabitethernet 1/0/4
[SwitchB-vlan4] igmp-snooping enable
[SwitchB-vlan4] quit
```

创建 VLAN 10，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchB] vlan 10
[SwitchB-vlan10] igmp-snooping enable
[SwitchB-vlan10] quit
```

配置端口 GigabitEthernet1/0/1 为 Hybrid 端口，并允许 VLAN 10 的报文带 Tag 通过。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type hybrid
[SwitchB-GigabitEthernet1/0/1] port hybrid vlan 10 tagged
[SwitchB-GigabitEthernet1/0/1] quit
```

配置 VLAN 10 为组播 VLAN，并把 VLAN 2～VLAN 4 都配置为该组播 VLAN 的子 VLAN。

```
[SwitchB] multicast-vlan 10
[SwitchB-mvlan-10] subvlan 2 to 4
[SwitchB-mvlan-10] quit
```

4. 验证配置

显示 Switch B 上所有组播 VLAN 的信息。

```
[SwitchB] display multicast-vlan
Total 1 multicast VLANs.

Multicast VLAN 10:
```

```
  Sub-VLAN list(3 in total):
     2-4
  Port list(0 in total):
```

显示 Switch B 上组播 VLAN 的所有组播组表项信息。

```
[SwitchB] display multicast-vlan group
Total 1 entries.

Multicast VLAN 10: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Sub-VLANs (3 in total):
      VLAN 2
      VLAN 3
      VLAN 4
```

由此可见，组播 VLAN（VLAN 10）在各子 VLAN（VLAN 2～VLAN 4）内维护组播组表项。

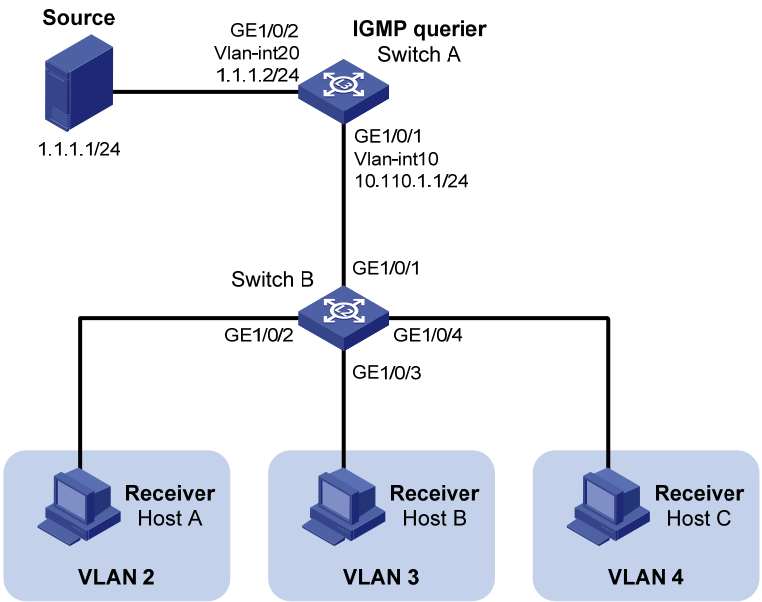
1.8.2 基于端口的组播VLAN配置举例

1. 组网需求

- 如 图 1-5 所示，三层交换机Switch A通过接口VLAN-interface20 连接组播源（Source），通过接口VLAN-interface10 连接二层交换机Switch B；Switch A上运行IGMPv2，Switch B上运行版本 2 的IGMP Snooping，并由Switch A充当IGMP查询器。
- 组播源向组播组 224.1.1.1 发送组播数据，Host A～Host C 都是该组播组的接收者（Receiver），且分别属于 VLAN 2～VLAN 4。
- 通过在 Switch B 上配置基于端口的组播 VLAN，使 Switch A 通过组播 VLAN 向 Switch B 下分属不同用户 VLAN 的主机分发组播数据。

2. 组网图

图1-5 基于端口的组播 VLAN 配置组网图



3. 配置步骤

(1) 配置 Switch A

使能 IP 组播路由。

```
<SwitchA> system-view
[SwitchA] multicast routing
[SwitchA-mrib] quit
```

创建 VLAN 20，并将端口 GigabitEthernet1/0/2 加入该 VLAN。

```
[SwitchA] vlan 20
[SwitchA-vlan20] port gigabitethernet 1/0/2
[SwitchA-vlan20] quit
```

在接口 VLAN-interface20 上配置 IP 地址，并使能 PIM-DM。

```
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ip address 1.1.1.2 24
[SwitchA-Vlan-interface20] pim dm
[SwitchA-Vlan-interface20] quit
```

创建 VLAN 10，将端口 GigabitEthernet1/0/1 加入该 VLAN。

```
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/1
[SwitchA-vlan10] quit
```

在接口 VLAN-interface10 上配置 IP 地址，并使能 IGMP。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ip address 10.110.1.1 24
[SwitchA-Vlan-interface10] igmp enable
[SwitchA-Vlan-interface10] quit
```

(2) 配置 Switch B

开启设备的 IGMP Snooping。

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

创建 VLAN 10，将端口 GigabitEthernet1/0/1 加入该 VLAN，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchB] vlan 10
[SwitchB-vlan10] port gigabitethernet 1/0/1
[SwitchB-vlan10] igmp-snooping enable
[SwitchB-vlan10] quit
```

创建 VLAN 2，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchB] vlan 2
[SwitchB-vlan2] igmp-snooping enable
[SwitchB-vlan2] quit
```

创建 VLAN 3，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchB] vlan 3
[SwitchB-vlan3] igmp-snooping enable
[SwitchB-vlan3] quit
```

创建 VLAN 4，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchB] vlan 4
```

```
[SwitchB-vlan4] igmp-snooping enable
[SwitchB-vlan4] quit
```

配置端口 GigabitEthernet1/0/2 为 Hybrid 类型，缺省 VLAN 为 VLAN 2；允许 VLAN 2 和 VLAN 10 的报文不带 Tag 通过。

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type hybrid
[SwitchB-GigabitEthernet1/0/2] port hybrid pvid vlan 2
[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 2 untagged
[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/2] quit
```

配置端口 GigabitEthernet1/0/3 为 Hybrid 类型，缺省 VLAN 为 VLAN 3；允许 VLAN 3 和 VLAN 10 的报文不带 Tag 通过。

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-type hybrid
[SwitchB-GigabitEthernet1/0/3] port hybrid pvid vlan 3
[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 3 untagged
[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/3] quit
```

配置端口 GigabitEthernet1/0/4 为 Hybrid 类型，缺省 VLAN 为 VLAN 4；允许 VLAN 4 和 VLAN 10 的报文不带 Tag 通过。

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] port link-type hybrid
[SwitchB-GigabitEthernet1/0/4] port hybrid pvid vlan 4
[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 4 untagged
[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/4] quit
```

配置 VLAN 10 为组播 VLAN。

```
[SwitchB] multicast-vlan 10
```

将端口 GigabitEthernet1/0/2 到 GigabitEthernet1/0/3 加入组播 VLAN 10。

```
[SwitchB-mvlan-10] port gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[SwitchB-mvlan-10] quit
```

配置端口 GigabitEthernet1/0/4 也属于组播 VLAN 10。

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] port multicast-vlan 10
[SwitchB-GigabitEthernet1/0/4] quit
```

4. 验证配置

显示 Switch B 上所有组播 VLAN 的信息。

```
[SwitchB] display multicast-vlan
Total 1 multicast VLANs.

Multicast VLAN 10:
  Sub-VLAN list(0 in total):
  Port list(3 in total):
    GE1/0/2
    GE1/0/3
    GE1/0/4
```

显示 Switch B 上动态组播组的 IGMP Snooping 转发表项信息。

```
[SwitchB] display igmp-snooping group
Total 1 entries.

VLAN 10: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host slots (0 in total):
    Host ports (3 in total):
      GE1/0/2        (00:03:23)
      GE1/0/3        (00:04:07)
      GE1/0/4        (00:04:16)
```

由此可见，IGMP Snooping 统一在组播 VLAN（VLAN 10）中维护成员端口。

目 录

1 MLD Snooping

1.1 MLD Snooping简介

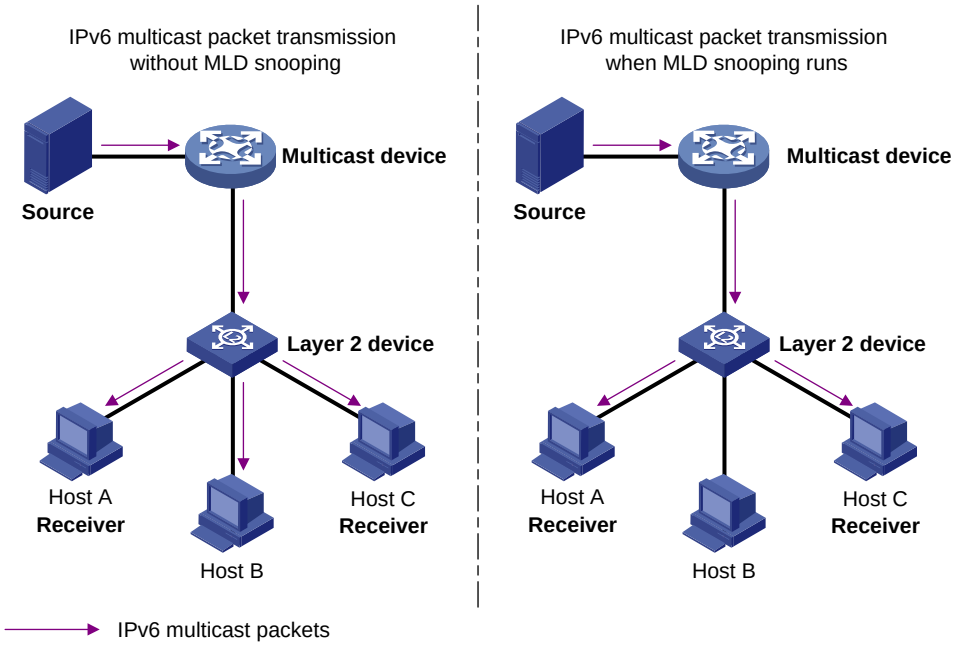
MLD Snooping（Multicast Listener Discovery Snooping，组播侦听者发现协议窥探）运行在二层设备上，通过侦听三层设备与主机之间的 MLD 报文来生成二层组播转发表，从而管理和控制 IPv6 组播数据报文的转发，实现 IPv6 组播数据报文在二层的按需分发。

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



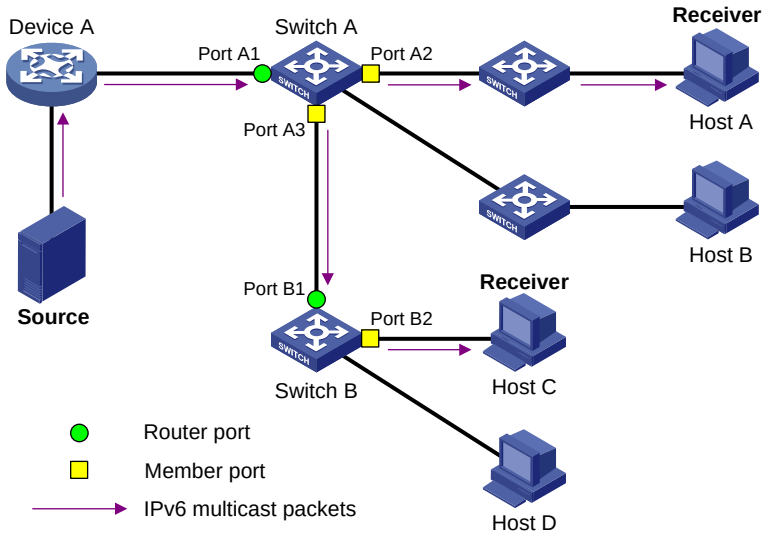
MLD Snooping 通过二层组播将信息只转发给有需要的接收者，可以带来以下好处：

- 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端口分类

如 图 1-2 所示，Device 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）。根据在网络中所处位置的不同，我们将MLD Snooping端口分为路由器端口和成员端口两类，以下分别介绍。

图1-2 MLD Snooping 端口示意图



1. 路由器端口

在运行了MLD Snooping的二层设备上，朝向上游三层组播设备的端口称为路由器端口。如 图 1-2 中Switch A的Port A1 端口和Switch B的Port B1 端口。

根据来源不同，路由器端口可分为：

- 动态路由器端口：所有收到 MLD 普遍组查询报文（源地址非 0::0）或 IPv6 PIM Hello 报文的端口，都被维护为动态路由器端口。这些端口被记录在动态路由器端口列表中，每个端口都有一个老化定时器。在老化定时器超时前，动态路由器端口如果收到了 MLD 普遍组查询报文（源地址非 0::0）或 IPv6 PIM Hello 报文，该定时器将被重置；否则，该端口将被从动态路由器端口列表中删除。
- 静态路由器端口：通过命令行手工配置的路由器端口称为静态路由器端口，这些端口被记录在静态路由器端口列表中。静态路由器端口只能通过命令行手工删除，不会被老化。

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。如果没有特别指明，本文中提到的路由器端口包括动态路由器端口和静态路由器端口。

---

2. 成员端口

在运行了MLD Snooping的二层设备上，朝向下游组播组成员的端口称为成员端口。如 图 1-2 中Switch A的Port A2 和Port A3 端口，以及Switch B的Port B2 端口。

根据来源不同，成员端口也可分为：

- 动态成员端口：所有收到 MLD 成员关系报告报文的端口，都被维护为动态成员端口。这些端口被记录在动态 MLD Snooping 转发表中，每个端口都有一个老化定时器。在老化定时器超时前，动态成员端口如果收到了 MLD 成员关系报告报文，该定时器将被重置；否则，该端口将被从动态 MLD Snooping 转发表中删除。
- 静态成员端口：通过命令行手工配置的成员端口称为静态成员端口，这些端口被记录在静态 MLD Snooping 转发表中。静态路由器端口只能通过命令行手工删除，不会被老化。

说明

如果没有特别指明，本文中提到的成员端口包括动态成员端口和静态成员端口。

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“1.7.2 配置静态成员端口” 和“1.7.3 配置静态路由器端口”。

1. 普遍组查询

MLD 查询器定期向本地网段内的所有主机与设备（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：

- 如果在动态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。
- 如果在动态路由器端口列表中尚未包含该动态路由器端口，则将其添加到动态路由器端口列表中，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。

说明

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。

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除该端口还有别的成员端口存在，二层设备不会向任何端口转发该报文，而将其直接丢弃。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，而是向该端口发送 MLD 特定组查询报文，并根据 MLD 特定组查询报文调整该端口的老化定时器（老化时间为 2×MLD 特定组查询报文的发送间隔）；
- 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只有该端口，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，而是向该端口发送 MLD 特定组查询报文，并根据 MLD 特定组查询报文调整该端口的老化定时器（老化时间为 2×MLD 特定组查询报文的发送间隔）。

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：

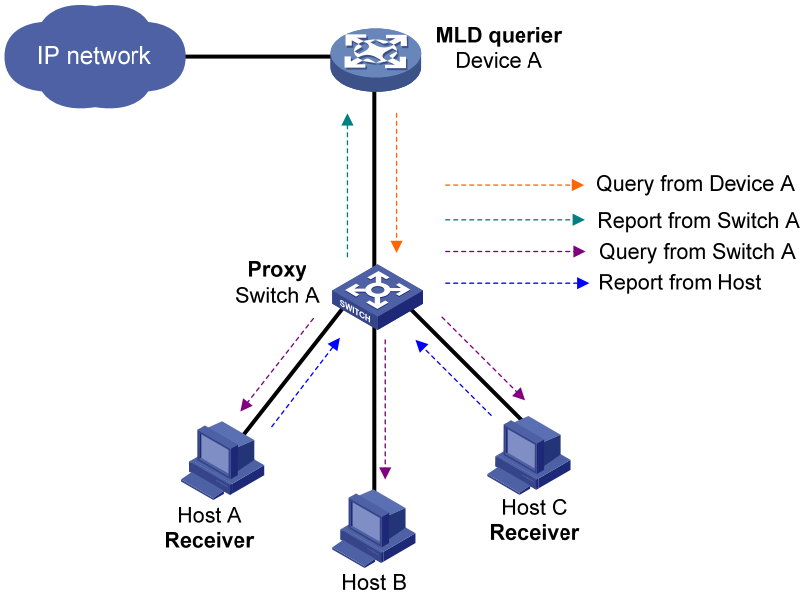
- 如果从该端口收到了主机响应该特定组查询的 MLD 成员关系报告报文，则表示该端口下还有该 IPv6 组播组的成员，于是重置其老化定时器；
- 如果没有从该端口收到主机响应该特定组查询的 MLD 成员关系报告报文，则表示该端口下已没有该 IPv6 组播组的成员。当该端口的老化定时器超时后，将其从该 IPv6 组播组所对应转发表项的出端口列表中删除。

1.1.4 MLD Snooping Proxy

为了减少上游设备收到的 MLD 报告报文和离开报文的数量，可以通过在边缘设备上配置 MLD Snooping Proxy（MLD Snooping 代理）功能，使其能够代理下游主机向上游设备发送报告报文和离开报文。配置了 MLD Snooping Proxy 功能的设备称为 MLD Snooping 代理设备，在其上游设备

看来，它就相当于一台主机。但主机上的 MLD 成员关系报告抑制机制在 MLD Snooping 代理设备上并不会生效。

图1-3 MLD Snooping Proxy 组网图



如 图 1-3 所示，作为MLD Snooping代理设备的Switch A，对其上游的MLD查询器Device A来说相当于一台主机，代理下游主机向Device A发送报告报文和离开报文。

MLD Snooping代理设备对MLD报文的处理方式如 表 1-1 所示。

表1-1 MLD Snooping 代理设备对 MLD 报文的处理方式

MLD 报文	处理方式
普遍组查询报文	收到普遍组查询报文后，向本VLAN内除接收端口以外的所有端口转发；同时根据本地维护的组成员关系生成报告报文，并向所有路由器端口发送
特定组/特定源组查询报文	收到针对某组播组的特定组/特定源组查询报文时，向本VLAN内除接收端口以外的所有路由器端口转发；若该组对应的转发表项中还有成员端口，则向本VLAN内所有路由器端口回复该组的报告报文
报告报文	从某端口收到某IPv6组播组的报告报文时，若已存在该组对应的转发表项，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；若已存在该组对应的转发表项，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；若尚不存在该组对应的转发表项，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，然后向所有路由器端口发送该组的报告报文
离开报文	从某端口收到某IPv6组播组的离开报文后，向该端口发送针对该组的特定组查询报文。只有当删除某IPv6组播组对应转发表项中的最后一个成员端口时，才会向所有路由器端口发送该组的离开报文

1.1.5 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配置限制和指导

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 中配置既可，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“Private 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。

对于既可在 VLAN 视图下配置，又可在 MLD-Snooping 视图下对多个 VLAN 进行配置的功能，两个视图下配置的优先级相同，最新配置生效。

对于既可在 VLAN 视图下配置，又可在 MLD-Snooping 视图下对所有 VLAN 配置的功能，VLAN 视图下的配置的优先级较高。

对于既可在接口视图下配置，又可在 MLD-Snooping 视图下配置的功能，MLD-Snooping 视图下的配置对指定 VLAN 内的所有端口生效，接口视图下配置只对当前接口生效，且接口视图下的配置优先级较高。

1.3 基于VLAN的MLD Snooping配置任务简介

基于 VLAN 的 MLD Snooping 的配置任务如下：

(1) 开启设备的MLD Snooping特性

(2) 使能MLD Snooping

请至少选择以下一项任务进行配置：

- 使能全局MLD Snooping
- 使能VLAN的MLD Snooping

(3) （可选）配置MLD Snooping基本功能

- 配置MLD Snooping版本
- 配置MLD Snooping转发表项的全局最大数量
- 配置IPv6 静态组播MAC地址表项
- 配置MLD特定组查询报文的发送间隔

(4) （可选）配置MLD Snooping端口功能

- 配置动态端口老化定时器
- 配置静态成员端口
- 配置静态路由器端口
- 配置模拟主机加入
- 配置端口快速离开功能
- 禁止端口成为动态路由器端口

(5) （可选）配置MLD Snooping查询器

- 开启MLD Snooping查询器
- 开启MLD Snooping查询器选举功能
- 配置MLD普遍组查询和响应

(6) （可选）配置MLD Snooping Proxy

(7) （可选）调整MLD报文

- 配置MLD报文的源IPv6 地址
- 配置MLD报文的 802.1p优先级

(8) （可选）配置MLD Snooping策略

- 配置IPv6 组播组过滤器
- 配置IPv6 组播数据报文源端口过滤
- 配置丢弃未知IPv6 组播数据报文
- 配置MLD成员关系报告报文抑制
- 配置端口加入的IPv6 组播组最大数量
- 配置IPv6 组播组替换功能
- 配置MLD Snooping主机跟踪功能
- 配置IPv6 组播用户控制策略

(9) （可选）配置设备发送的MLD协议报文的DSCP优先级

1.4 开启设备的MLD Snooping特性

1. 功能简介

只有在开启了设备的 MLD Snooping 特性后，才能进行其它的 MLD Snooping 相关配置。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启设备的 MLD Snooping 特性，并进入 MLD-Snooping 视图。

mld-snooping

缺省情况下，设备的 MLD Snooping 特性处于关闭状态。

1.5 使能MLD Snooping

1.5.1 使能全局MLD Snooping

1. 功能简介

使能全局 MLD Snooping 后，设备上所有 VLAN 的 MLD Snooping 都将使能。如果某个 VLAN 内不需要使用 MLD Snooping，可以在其中关闭 MLD snooping。

2. 配置限制和指导

使能全局 MLD Snooping 后，若还需在某指定 VLAN 内配置其他 MLD Snooping 功能，则必须在这些 VLAN 下使能 MLD Snooping，否则配置的其他 MLD Snooping 功能不生效。

使能或关闭 VLAN 内的 MLD Snooping 的优先级高于使能全局 MLD Snooping。例如：使能全局 MLD Snooping 后，再在某 VLAN 视图下通过 **mld-snooping disable** 命令关闭当前 VLAN 的 MLD Snooping，则该 VLAN 内的 MLD Snooping 处于关闭状态。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 MLD-Snooping 视图。

mld-snooping

(3) 使能全局 MLD Snooping。

global-enable

缺省情况下，全局 MLD Snooping 处于关闭状态。

(4) （可选）关闭某 VLAN 的 MLD Snooping。

a. 退回系统视图。

quit

b. 进入 VLAN 视图。

vlan *vlan-id*

c. 关闭该 VLAN 的 MLD Snooping。

mld-snooping disable

缺省情况下，VLAN 内 MLD Snooping 的状态与全局 MLD Snooping 的状态保持一致。

1.5.2 使能VLAN的MLD Snooping

1. 配置限制和指导

用户既可在 MLD-Snooping 视图下对单个或多个 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。

在 VLAN 内使能了 MLD Snooping 之后，MLD Snooping 只在属于该 VLAN 的端口上生效。

2. 使能单个或多个VLAN的MLD Snooping

(1) 进入系统视图。

system-view

(2) 进入 MLD-Snooping 视图。

mld-snooping

(3) 使能单个或多个 VLAN 的 MLD Snooping。

enable vlan *vlan-list*

缺省情况下，VLAN 内 MLD Snooping 的状态与全局 MLD Snooping 的状态保持一致。

3. 使能单个VLAN的MLD Snooping

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 使能该 VLAN 的 MLD Snooping。

mld-snooping enable

缺省情况下，VLAN 内 MLD Snooping 的状态与全局 MLD Snooping 的状态保持一致。

1.6 配置MLD Snooping基本功能

1.6.1 配置MLD Snooping版本

1. 功能简介

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 的报文和 MLDv2 的查询报文进行处理，对 MLDv2 的成员关系报文则不进行处理，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。

2. 配置限制和指导

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“1.7.2 配置静态成员端口”。

3. 配置多个VLAN内的MLD Snooping版本

(1) 进入系统视图。

system-view

(2) 进入 MLD-Snooping 视图。

mld-snooping

(3) 配置指定 VLAN 内的 MLD Snooping 的版本。

version *version-number* **vlan** *vlan-list*

缺省情况下，VLAN 内 MLD Snooping 的版本为 1。

4. 配置单个VLAN内的MLD Snooping版本

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 在 VLAN 内配置 MLD Snooping 的版本。

mld-snooping version *version-number*

缺省情况下，VLAN 内 MLD Snooping 的版本为 1。

1.6.2 配置MLD Snooping转发表项的全局最大数量

1. 功能简介

用户可以调整 MLD Snooping 转发表项（包括动态表项和静态表项）的全局最大数量，当设备上维护的表项数量达到或超过最大数量后，系统不再创建新的表项，也不会主动删除多余表项，直至有表项被老化或被手工删除，所以当设备上维护的表项数量达到或超过最大数量后，为避免此后无法再创建新的表项，建议用户手工删除多余表项。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 MLD-Snooping 视图。

mld-snooping

(3) 配置 MLD Snooping 转发表项的全局最大数量。

entry-limit *limit*

缺省情况下，MLD Snooping 转发表项的全局最大数量为 4294967295。

1.6.3 配置IPv6 静态组播MAC地址表项

1. 功能简介

在二层组播中，除了可通过二层 IPv6 组播协议（如 MLD Snooping）动态建立 IPv6 组播 MAC 地址表项外，还可通过手工方式配置 IPv6 组播 MAC 地址表项，将端口与 IPv6 组播 MAC 地址进行静态绑定，以便灵活控制 IPv6 组播信息送达的目的端口。

2. 配置限制和指导

可手工配置的组播 MAC 地址表项必须是尚未使用的组播 MAC 地址（即最高字节的最低比特位为 1 的 MAC 地址）。

3. 系统视图下配置IPv6 静态组播MAC地址表项

(1) 进入系统视图。

system-view

(2) 配置静态组播 MAC 地址表项。

mac-address multicast *mac-address* **interface** *interface-list* **vlan** *vlan-id*

4. 接口视图下配置IPv6 静态组播MAC地址表项

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 配置静态组播 MAC 地址表项。

mac-address multicast *mac-address* **vlan** *vlan-id*

1.6.4 配置MLD特定组查询报文的发送间隔

1. 功能简介

合理配置 MLD 特定组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。

二层设备所发送的 MLD 特定组查询报文，其报文的最大响应时间字段由所配置的 MLD 特定组查询报文的发送间隔来填充，在主机在收到 MLD 特定组查询报文后，会为其所加入的该 IPv6 组播组启动一个定时器，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 特定组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。

2. 全局配置MLD特定组查询报文的发送间隔

(1) 进入系统视图。

system-view

(2) 进入 MLD-Snooping 视图。

mld-snooping

(3) 全局配置 MLD 特定组查询报文的发送间隔。

last-listener-query-interval *interval*

缺省情况下，MLD 特定组查询报文的发送间隔为 1 秒。

3. 在VLAN内配置MLD特定组查询报文的发送间隔

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 在 VLAN 内配置 MLD 特定组查询报文的发送间隔。

mld-snooping last-listener-query-interval *interval*

缺省情况下，MLD 特定组查询报文的发送间隔为 1 秒。

1.7 配置MLD Snooping端口功能

1.7.1 配置动态端口老化定时器

1. 功能简介

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动态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。

2. 配置限制和指导

- 请根据网络环境合理设置动态端口的老化时间，比如网络中 IPv6 组播组成员变动比较频繁，可以把动态成员端口老化时间设置小一些，避免一些无效表项老化时间过长。
- 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。
- 如果二层设备向动态成员端口主动发送MLD特定组查询报文，则该端口的老化时间将根据该MLD特定组查询报文进行调整，调整的老化时间为 2×MLD特定组查询报文的发送间隔。二层设备MLD特定组查询报文发送间隔的配置，请参见“1.6.4 配置MLD特定组查询报文的发送间隔”。

3. 全局配置动态端口老化定时器

(1) 进入系统视图。

system-view

(2) 进入 MLD-Snooping 视图。

mld-snooping

(3) 全局配置动态路由器端口老化时间。

router-aging-time *seconds*

缺省情况下，动态路由器端口的老化时间为 260 秒。

(4) 全局配置动态成员端口老化时间。

host-aging-time *seconds*

缺省情况下，动态成员端口的老化时间为 260 秒。

4. 在VLAN内配置动态端口老化定时器

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 在 VLAN 内配置动态路由器端口老化时间。

mld-snooping router-aging-time *seconds*

缺省情况下，动态路由器端口的老化时间为 260 秒。

(4) 在 VLAN 内配置动态成员端口老化时间。

mld-snooping host-aging-time *seconds*

缺省情况下，动态成员端口的老化时间为 260 秒。

1.7.2 配置静态成员端口

1. 功能简介

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。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 配置静态成员端口。

mld-snooping static-group *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

缺省情况下，端口不是静态成员端口。

1.7.3 配置静态路由器端口

1. 功能简介

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

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 配置静态路由器端口。

mld-snooping static-router-port vlan *vlan-id*

缺省情况下，端口不是静态路由器端口。

1.7.4 配置模拟主机加入

1. 功能简介

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。

在二层设备的端口上配置了模拟主机加入后，模拟主机所采用的 MLD 版本与 MLD Snooping 的版本一致，并且该端口将作为动态成员端口参与动态成员端口的老化过程。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 配置模拟主机加入。

mld-snooping host-join *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

缺省情况下，未配置模拟主机加入。

1.7.5 配置端口快速离开功能

1. 功能简介

端口快速离开功能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，二层设备不会向该端口发送或转发针对该 IPv6 组播组的 MLD 特定组查询报文。

2. 配置限制和指导

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。

3. 全局配置端口快速离开功能

(1) 进入系统视图。

system-view

(2) 进入 MLD-Snooping 视图。

mld-snooping

(3) 全局开启端口快速离开功能。

fast-leave [**vlan** *vlan-list*]

缺省情况下，端口快速离开功能处于关闭状态。

4. 在端口上配置端口快速离开功能

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 在端口上开启端口快速离开功能。

mld-snooping fast-leave [**vlan** *vlan-list*]

缺省情况下，端口快速离开功能处于关闭状态。

1.7.6 禁止端口成为动态路由器端口

1. 功能简介

在 IPv6 组播用户接入网络中，用户主机在某些情况下（比如测试）也会发出 MLD 普遍组查询报文或 IPv6 PIM Hello 报文：

- 如果二层设备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，那么接收报文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，导致该主机收到大量无用的 IPv6 组播报文。
- 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。

当禁止一个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组播用户的控制能力。

2. 配置限制和指导

禁止端口成为动态路由器端口的配置与静态路由器端口的配置互不影响。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 禁止端口成为动态路由器端口。

mld-snooping router-port-deny [**vlan** *vlan-list*]

缺省情况下，端口可以成为动态路由器端口。

1.8 配置MLD Snooping查询器

1.8.1 开启MLD Snooping查询器

1. 功能简介

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，可以在二层设备上开启 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。

2. 配置限制和指导

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。

3. 在VLAN内开启MLD Snooping查询器

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 开启 MLD Snooping 查询器。

mld-snooping querier

缺省情况下，MLD Snooping 查询器处于关闭状态。

1.8.2 开启MLD Snooping查询器选举功能

1. 功能简介

为了避免某 VLAN 因单一 MLD Snooping 查询器发生故障引起组播业务中断，建议在 VLAN 内配置多个 MLD Snooping 查询器，各设备上开启 MLD Snooping 查询器选举功能。当选举出的 MLD Snooping 查询器发生故障无法正常工作后，VLAN 内各设备会重新选举出新的 MLD Snooping 查询器以保证组播业务正常转发。MLD snooping 查询器选举机制和 MLD 查询器选举机制一样。

2. 配置准备

在VLAN内开启MLD Snooping查询器选举功能之前，需要先开启MLD Snooping查询器。有关开启MLD Snooping查询器的详细介绍，请参见“1.8.1 开启MLD Snooping查询器”

由于 MLD Snooping 查询器收到源 IPv6 地址为::的查询报文和源 IPv6 地址与本机查询器 IPv6 地址相同的查询报文不进行选举，因此，用户需要通过 **mld-snooping general-query source-ip** 配置将 MLD 查询报文的源 IPv6 地址配置为一个未被其他设备和主机使用的有效 IPv6 地址以避免上述问题。

通过 **mld-snooping version** 命令保证参与 MLD Snooping 查询器选举的各设备 MLD Snooping 版本相同。

3. 在VLAN内开启MLD Snooping查询器选举功能

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 开启 MLD Snooping 查询器选举功能。

mld-snooping querier-election

缺省情况下，VLAN 内 MLD Snooping 查询器选举功能处于关闭状态。

1.8.3 配置MLD普遍组查询和响应

1. 功能简介

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。

合理配置 MLD 普遍组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，其报文最大响应时间字段由所配置的 MLD 普遍组查询的最大响应时间来填充，在主机收到 MLD 普遍组查询报文后，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 普遍组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。

2. 配置限制和指导

为避免误删 IPv6 组播组成员，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。

3. 全局配置MLD普遍组查询和响应

(1) 进入系统视图。

system-view

(2) 进入 MLD-Snooping 视图。

mld-snooping

(3) 全局配置 MLD 普遍组查询的最大响应时间。

max-response-time *seconds*

缺省情况下，MLD 普遍组查询的最大响应时间为 10 秒。

4. 在VLAN内配置MLD普遍组查询和响应

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 在 VLAN 内配置 MLD 普遍组查询报文的发送间隔。

mld-snooping query-interval *interval*

缺省情况下，MLD 普遍组查询报文的发送间隔为 125 秒。

(4) 在 VLAN 内配置 MLD 普遍组查询的最大响应时间。

mld-snooping max-response-time *seconds*

缺省情况下，MLD 普遍组查询的最大响应时间为 10 秒。

1.9 配置MLD Snooping Proxy

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 在 VLAN 内开启 MLD Snooping Proxy 功能。

mld-snooping proxy enable

缺省情况下，VLAN 内的 MLD Snooping Proxy 功能处于关闭状态。

1.10 调整MLD报文

1.10.1 配置MLD报文的源IPv6 地址

1. 功能简介

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。如果本网段内存在别的 MLD 查询器，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。

用户也可以改变模拟主机或 MLD Snooping 代理发送的 MLD 成员关系报告报文或 MLD 离开组报文的源 IPv6 地址。

2. 在VLAN内配置MLD报文的源IPv6 地址

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 配置 MLD 普遍组查询报文的源 IPv6 地址。

mld-snooping general-query source-ip *ipv6-address*

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。

(4) 配置 MLD 特定组查询报文的源 IPv6 地址。

mld-snooping special-query source-ip *ipv6-address*

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。

(5) 配置 MLD 成员关系报告报文的源 IPv6 地址。

mld-snooping report source-ip *ipv6-address*

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。

(6) 配置 MLD 离开组报文的源 IPv6 地址。

mld-snooping done source-ip *ipv6-address*

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。

1.10.2 配置MLD报文的 802.1p优先级

1. 功能简介

当二层设备的出端口发生拥塞时，二层设备通过识别报文的 802.1p 优先级，优先发送优先级较高的报文。用户可以通过本配置改变 MLD 报文（包括本设备生成的以及途经本设备的）的 802.1p 优先级。

2. 全局配置MLD报文的 802.1p优先级

(1) 进入系统视图。

system-view

(2) 进入 MLD-Snooping 视图。

mld-snooping

(3) 全局配置 MLD 报文的 802.1p 优先级。

dot1p-priority *priority*

缺省情况下，MLD 报文的 802.1p 优先级为 6。

3. 在VLAN内配置MLD报文的 802.1p优先级

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 在 VLAN 内配置 MLD 报文的 802.1p 优先级。

mld-snooping dot1p-priority *priority*

缺省情况下，VLAN 内 MLD 报文的 802.1p 优先级为 6。

1.11 配置MLD Snooping策略

1.11.1 配置IPv6 组播组过滤器

1. 功能简介

在使能了 MLD Snooping 的二层设备上，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。本配置只对动态组播组有效，对静态组播组无效。

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，该报文将在二层设备上接受 IPv6 组播组过滤器的检查，只有通过了检查，二层设备才会将该主机所属的端口加入到出端口列表中，从而达到控制用户点播组播节目的目的。

2. 全局配置IPv6 组播组过滤器

(1) 进入系统视图。

system-view

(2) 进入 MLD-Snooping 视图。

mld-snooping

(3) 全局配置 IPv6 组播组过滤器。

group-policy *ipv6-acl-number* [**vlan** *vlan-list*]

缺省情况下，未配置 IPv6 组播组过滤器，即主机可以加入任意合法的 IPv6 组播组。

3. 在端口上配置IPv6 组播组过滤器

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 在端口上配置 IPv6 组播组过滤器。

mld-snooping group-policy *ipv6-acl-number* [**vlan** *vlan-list*]

缺省情况下，未配置 IPv6 组播组过滤器，即主机可以加入任意合法的 IPv6 组播组。

1.11.2 配置IPv6 组播数据报文源端口过滤

1. 功能简介

通过配置 IPv6 组播数据报文源端口过滤功能，可以允许或禁止端口作为 IPv6 组播源端口：

- 开启该功能后，端口不能连接 IPv6 组播源，因为该端口将过滤掉所有的 IPv6 组播数据报文（但允许 IPv6 组播协议报文通过），因此只能连接 IPv6 组播数据接收者。
- 关闭该功能后，端口既能连接 IPv6 组播源，也能连接 IPv6 组播数据接收者。

2. 配置限制和指导

在开启 IPv6 组播数据报文源端口过滤功能时，系统将同时开启 IPv4 组播数据报文源端口过滤功能。

配置 IPv6 组播数据报文源端口过滤在全局配置或在端口上配置的优先级相同，最新配置生效。

3. 全局配置IPv6 组播数据报文源端口过滤

(1) 进入系统视图。

system-view

(2) 进入 MLD-Snooping 视图。

mld-snooping

(3) 开启指定端口的 IPv6 组播数据报文源端口过滤功能。

source-deny port *interface-list*

缺省情况下，IPv6 组播数据报文源端口过滤功能处于关闭状态。

4. 在端口上配置IPv6 组播数据报文源端口过滤

(1) 进入系统视图。

system-view

(2) 进入二层以太网接口视图。

interface *interface-type interface-number*

(3) 开启当前端口的 IPv6 组播数据报文源端口过滤功能。

mld-snooping source-deny

缺省情况下，IPv6 组播数据报文源端口过滤功能处于关闭状态。

1.11.3 配置丢弃未知IPv6 组播数据报文

1. 功能简介

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：

- 当开启了丢弃未知 IPv6 组播数据报文功能时，二层设备只向其路由器端口转发未知 IPv6 组播数据报文，不在 VLAN 内广播；如果二层设备没有路由器端口，未知 IPv6 组播数据报文报文会被丢弃，不再转发。
- 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。

2. 配置指导和限制

在开启了丢弃未知 IPv6 组播数据报文功能之后，未知 IPv4 组播数据报文也将被丢弃。

在开启了丢弃未知IPv6 组播数据报文的功能之后，仍会向 VLAN 内的其它路由器端口转发未知IPv6 组播数据报文。

3. 在VLAN内配置丢弃未知IPv6 组播数据报文

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 在 VLAN 内开启丢弃未知 IPv6 组播数据报文功能。

mld-snooping drop-unknown

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。

1.11.4 配置MLD成员关系报告报文抑制

1. 功能简介

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。

当开启了 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。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 MLD-Snooping 视图。

mld-snooping

(3) 开启 MLD 成员关系报告报文抑制功能。

report-aggregation

缺省情况下，MLD 成员关系报告报文抑制功能处于开启状态。

1.11.5 配置端口加入的IPv6 组播组最大数量

1. 功能简介

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。本配置只对动态组播组有效，对静态组播组无效。

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，系统将自动丢弃新的 MLD 成员关系报告报文。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 配置端口加入的 IPv6 组播组最大数量。

mld-snooping group-limit *limit* [**vlan** *vlan-list*]

缺省情况下，未对端口加入的 IPv6 组播组最大数量进行限制。

1.11.6 配置IPv6 组播组替换功能

1. 功能简介

当端口上的 IPv6 组播组数目达到配置端口加入的 IPv6 组播组最大数量时，会自动丢弃新的 MLD 成员关系报告报文。IPv6 组播组替换功能开启后，当端口收到新的 MLD 成员关系报告报文时，会自动离开 IPv6 地址最小的 IPv6 组播组并加入新的 IPv6 组播组。该特性的典型应用就是频道切换。用户切换频道时，就是离开一个 IPv6 组播组并加入到新的 IPv6 组播组。

2. 配置限制和指导

本配置只对动态组播组有效，对静态组播组无效。

当设备上维护的 MLD Snooping 转发表项达到配置的 MLD Snooping 转发表项的全局最大数量并且端口新加入的 IPv6 组播组不在设备维护的 IPv6 组播组列表中时，IPv6 组播组替换功能不能生效。

3. 全局配置IPv6 组播组替换功能

(1) 进入系统视图。

system-view

(2) 进入 MLD-Snooping 视图。

mld-snooping

(3) 全局开启 IPv6 组播组替换功能。

overflow-replace [**vlan** *vlan-list*]

缺省情况下，IPv6 组播组替换功能处于关闭状态。

4. 在端口上配置IPv6 组播组替换功能

(1) 进入系统视图。

system-view

(2) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 在端口上开启 IPv6 组播组替换功能。

mld-snooping overflow-replace [**vlan** *vlan-list*]

缺省情况下，IPv6 组播组替换功能处于关闭状态。

1.11.7 配置MLD Snooping主机跟踪功能

1. 功能简介

通过开启 MLD Snooping 主机跟踪功能，可以使二层设备能够记录正在接收 IPv6 组播数据的成员主机信息（包括主机的 IPv6 地址、加入 IPv6 组播组的运行时长和超时剩余时间等），以便于网络管理员对这些主机进行监控和管理。

2. 全局配置MLD Snooping主机跟踪功能

(1) 进入系统视图。

system-view

(2) 进入 MLD-Snooping 视图。

mld-snooping

(3) 全局开启 MLD Snooping 主机跟踪功能。

host-tracking

缺省情况下，MLD Snooping 主机跟踪功能处于关闭状态。

3. 在VLAN内配置MLD Snooping主机跟踪功能

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 在 VLAN 内开启 MLD Snooping 主机跟踪功能。

mld-snooping host-tracking

缺省情况下，MLD Snooping 主机跟踪功能处于关闭状态。

1.11.8 配置IPv6 组播用户控制策略

1. 功能简介

通过配置 IPv6 组播用户控制策略，设备可以对 IPv6 组播用户发送的 MLD 成员关系报文和 MLD 离开报文进行过滤，从而使设备只对策略所许可的 IPv6 组播组维护组播成员关系。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 User-Profile 视图。

user-profile *profile-name*

本命令的详细介绍请参见“安全配置指导”中的“User Profile”。

(3) 配置 IPv6 组播用户控制策略。

mld-snooping access-policy *ipv6-acl-number*

缺省情况下，不存在 IPv6 组播用户控制策略，即用户可以加入/离开任意合法的 IPv6 组播组

1.12 配置设备发送的MLD协议报文的DSCP优先级

1. 功能简介

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。通过本配置可以指定设备发送的 MLD 协议报文的 DSCP 优先级。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 MLD Snooping 视图。

mld-snooping

(3) 配置设备发送的 MLD 协议报文的 DSCP 优先级。

dscp *dscp-value*

缺省情况下，设备发送的 MLD 协议报文的 DSCP 优先级为 48。

1.13 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1-2 MLD Snooping 显示和维护

操作	命令
显示IPv6二层组播快速转发表信息	**display ipv6 l2-multicast fast-forwarding cache** [**vlan** *vlan-id*] [*ipv6-source-address* | *ipv6-group-address*] * [**slot** *slot-number*]
显示IPv6二层组播的IP组播组信息	**display ipv6 l2-multicast ip** [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]
显示IPv6二层组播的IP转发表信息	**display ipv6 l2-multicast ip forwarding** [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]
显示IPv6二层组播的MAC组播组信息	**display ipv6 l2-multicast mac** [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]
显示IPv6二层组播的MAC转发表信息	**display ipv6 l2-multicast mac forwarding** [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]
显示IPv6静态组播MAC地址表信息	**display mac-address** [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]]
显示MLD Snooping的状态信息	**display mld-snooping** [**global** | **vlan** *vlan-id*]
显示动态MLD Snooping IPv6组播组的信息	**display mld-snooping group** [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**interface** *interface-type interface-number* | [**verbose**] [**slot** *slot-number*]]
显示MLD Snooping 主机跟踪信息	**display mld-snooping host-tracking vlan** *vlan-id* **group** *ipv6-group-address* [**source** *ipv6-source-address*] [**slot** *slot-number*]
显示IPv6动态路由器端口的信息	**display mld-snooping router-port** [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
显示静态MLD Snooping IPv6组播组的信息	**display mld-snooping static-group** [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
显示IPv6静态路由器端口的信息	**display mld-snooping static-router-port** [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
显示MLD Snooping监听到的MLD报文和IPv6 PIM hello报文的统计信息	**display mld-snooping statistics**

操作	命令
清除IPv6二层组播快速转发表中的转发项	**reset ipv6 l2-multicast fast-forwarding cache** [**vlan** *vlan-id*] { { *ipv6-source-address* | *ipv6-group-address* } * | **all** } [**slot** *slot-number*]
清除动态MLD Snooping IPv6组播组的信息	**reset mld-snooping group** { *ipv6-group-address* [*ipv6-source-address*] | **all** } [**vlan** *vlan-id*]
清除IPv6动态路由器端口的信息	**reset mld-snooping router-port** { **all** | **vlan** *vlan-id* }
清除MLD Snooping监听到的MLD报文和IPv6 PIM hello报文的统计信息	**reset mld-snooping statistics**

1.14 MLD Snooping典型配置举例

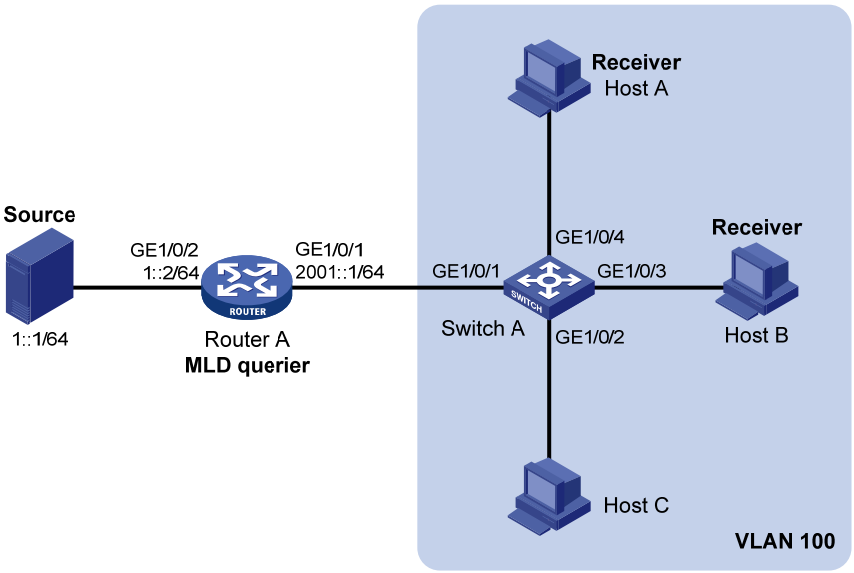
1.14.1 基于VLAN的IPv6 组策略及模拟主机加入配置举例

1. 组网需求

- 如 图 1-4 所示，Router A通过GigabitEthernet1/0/2 接口连接IPv6 组播源（Source），通过GigabitEthernet1/0/1 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 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 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 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1-4 基于 VLAN 的 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 1-4 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 GigabitEthernet1/0/2 上使能 IPv6 PIM-DM，并在接口 GigabitEthernet1/0/1 上使能 MLD。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ipv6 pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

(3) 配置 Switch A

开启设备的 MLD Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并开启丢弃未知 IPv6 组播数据报文功能。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[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 basic 2001
[SwitchA-acl-ipv6-basic-2001] rule permit source ff1e::101 128
[SwitchA-acl-ipv6-basic-2001] quit
[SwitchA] mld-snooping
[SwitchA–mld-snooping] group-policy 2001 vlan 100
[SwitchA–mld-snooping] quit
```

在 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 上分别配置模拟主机加入 IPv6 组播组 FF1E::101。

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet1/0/4] 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内动态MLD Snooping IPv6组播组的信息。

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

VLAN 100: Total 1 entries.
  (::, FF1E::101)
    Host ports (2 in total):
      GE1/0/3                              (00:03:23)
      GE1/0/4                              (00:04:10)
```

由此可见，Host A和Host B所在的端口GigabitEthernet1/0/4和GigabitEthernet1/0/3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。

1.14.2 基于VLAN的静态端口配置举例

1. 组网需求

- 如 图 1-5 所示，Router A通过GigabitEthernet1/0/2接口连接IPv6组播源（Source），通过GigabitEthernet1/0/1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GigabitEthernet1/0/3和GigabitEthernet1/0/5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GigabitEthernet1/0/3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

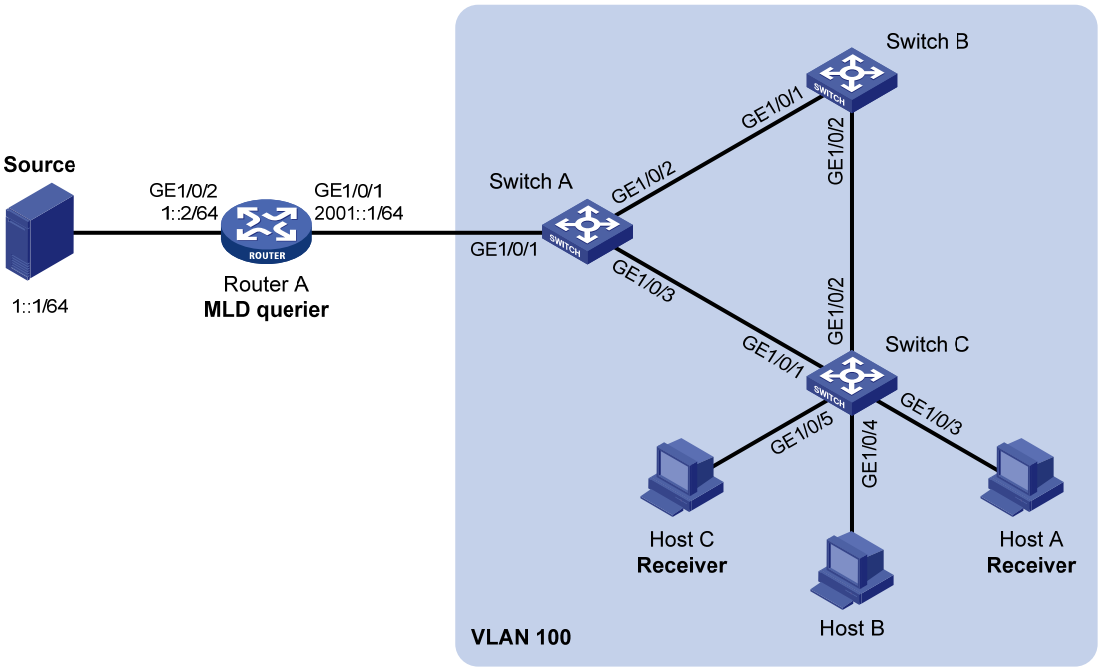
如果没有配置静态路由器端口，那么当Switch A—Switch B—Switch C的路径出现阻断时，至少需要等待一个MLD查询和响应周期完成后，IPv6组播数据才能通过Switch A—Switch C的新路径传递给接收者，IPv6组播数据的传输在这个过程中将中断。

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1-5 基于 VLAN 的静态端口配置组网图



3. 配置步骤

(1) 配置 IPv6 地址

请按照 图 1-5 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 GigabitEthernet1/0/2 上使能 IPv6 PIM-DM，并在接口 GigabitEthernet1/0/1 上使能 MLD。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ipv6 pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

(3) 配置 Switch A

开启设备的 MLD Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/3 添加到该 VLAN 中，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchA] vlan 100
```

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

把 GigabitEthernet1/0/3 配置为静态路由器端口。

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mld-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

(4) 配置 Switch B

开启设备的 MLD Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 添加到该 VLAN 中，并在该 VLAN 内使能 MLD Snooping。

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

(5) 配置 Switch C

开启设备的 MLD Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/5 添加到该 VLAN 中，并在该 VLAN 内使能 MLD Snooping。

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

分别在端口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/5 上配置静态加入 IPv6 组播组 FF1E::101。

```
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet1/0/3] quit
[SwitchC] interface gigabitethernet 1/0/5
[SwitchC-GigabitEthernet1/0/5] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet1/0/5] 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 ports (1 in total):
    GE1/0/3
```

由此可见，Switch A 上的端口 GigabitEthernet1/0/3 已经成为了静态路由器端口。

显示 Switch C 上 VLAN 100 内静态 MLD Snooping IPv6 组播组的信息。

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

VLAN 100: Total 1 entries.
  (::, FF1E::101)
    Host ports (2 in total):
      GE1/0/3
      GE1/0/5
```

由此可见，Switch C 上的端口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/5 已经成为了 IPv6 组播组 FF1E::101 的静态成员端口。

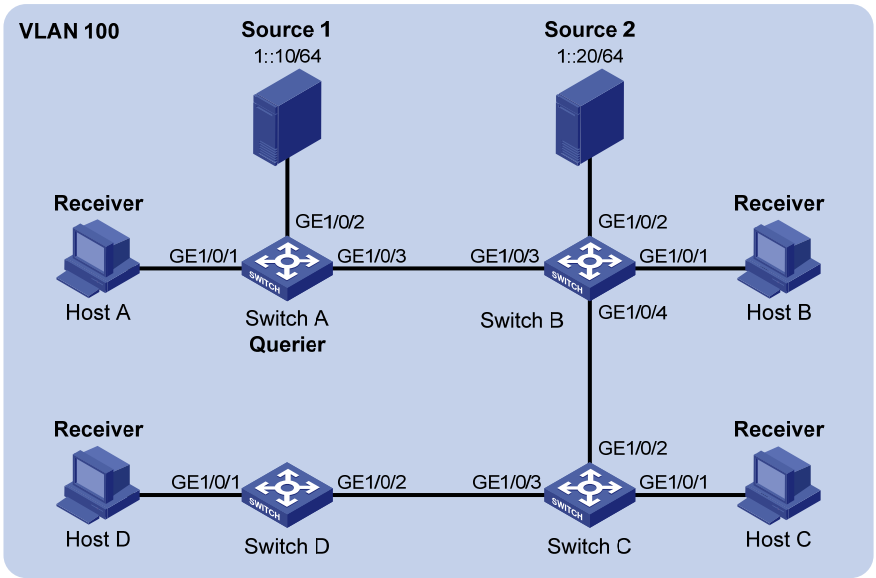
1.14.3 基于VLAN的MLD Snooping查询器配置举例

1. 组网需求

- 如 图 1-6 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 组播源较近的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，在所有交换机上都开启丢弃未知 IPv6 组播数据报文功能。

2. 组网图

图1-6 基于 VLAN 的 MLD Snooping 查询器配置组网图



3. 配置步骤

(1) 配置 Switch A

开启设备的 MLD Snooping 特性。

```
<SwitchA> system-view
```

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/3 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并开启丢弃未知 IPv6 组播数据报文功能。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[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

开启设备的 MLD Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并开启丢弃未知 IPv6 组播数据报文功能。

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

(3) 配置 Switch C

开启设备的 MLD Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/3 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并开启丢弃未知 IPv6 组播数据报文功能。

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

(4) 配置 Switch D

开启设备的 MLD Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/2 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并开启丢弃未知 IPv6 组播数据报文功能。

```
[SwitchD] vlan 100
[SwitchD-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[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 报文和 IPv6 PIM hello 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 IPv6 PIM hello:  0
Received error MLD messages:  0
```

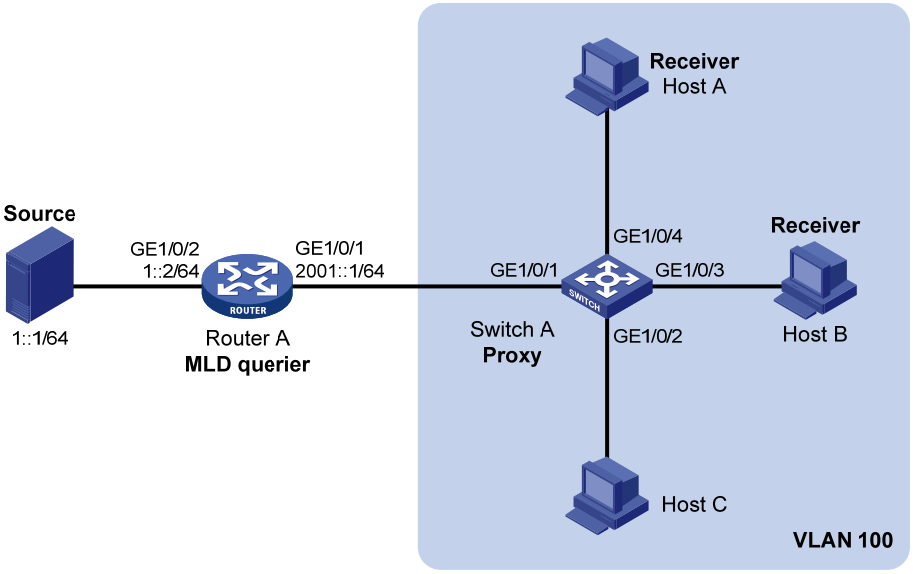
1.14.4 基于VLAN的MLD Snooping Proxy配置举例

1. 组网需求

- 如 图 1-7 所示，Router A通过GigabitEthernet1/0/2 接口连接IPv6 组播源（Source），通过GigabitEthernet1/0/1 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 Switch A 能够代理下游主机向 Router A 发送的 MLD 报告报文和离开报文，以及响应 Router A 发来的 MLD 查询报文并向下游主机转发。

2. 组网图

图1-7 基于 VLAN 的 MLD Snooping Proxy 配置组网图



3. 配置步骤

(1) 配置 IPv6 地址

使能各设备的 IPv6 转发功能，并按照配置各接口的 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 GigabitEthernet1/0/2 上使能 IPv6 PIM-DM，并在接口 GigabitEthernet1/0/1 上使能 MLD。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] ipv6 pim dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ipv6 pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

(3) 配置 Switch A

开启设备的 MLD Snooping 特性。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并使能 MLD Snooping Proxy。

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

```
[SwitchA-vlan100] mld-snooping proxy enable
[SwitchA-vlan100] quit
```

4. 验证配置

当配置完成后，Host A 和 Host B 分别发送组地址为 FF1E::101 的 MLD 加入报文，Switch A 收到该报文后通过其路由器端口 GigabitEthernet1/0/1 向 Router A 也发送该组的加入报文。通过使用 **display mld-snooping group** 和 **display mld group** 命令可以分别查看 MLD Snooping 组和 MLD 组的信息，例如：

查看 Switch A 上 MLD Snooping IPv6 组播组的信息。

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

VLAN 100: Total 1 entries.
  (::, FF1E::101)
    Host ports (2 in total):
      GE1/0/3                                  (00:04:09)
      GE1/0/4                                  (00:03:06)
```

查看 Router A 上 MLD 组的信息。

```
[RouterA] display mld group
MLD groups in total: 1
 GigabitEthernet1/0/1(2001::1):
  MLD groups reported in total: 1
   Group address: FF1E::101
    Last reporter: FE80::2FF:FFFF:FE00:1
    Uptime: 00:00:31
    Expires: 00:03:48
```

当 Host A 离开 IPv6 组播组 FF1E::101 时，向 Switch A 发送该组的 MLD 离开报文，但由于 Host B 仍未离开该组，因此 Switch A 并不会删除该组，也不会向 Router A 发送该组的离开报文，只是在该组对应转发表项的成员端口列表中将端口 GigabitEthernet1/0/4 删除。通过使用 **display mld-snooping group** 命令可以查看 MLD Snooping 组的信息，例如：

查看 Switch A 上 MLD Snooping IPv6 组播组的信息。

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

VLAN 100: Total 1 entries.
  (::, FF1E::101)
    Host ports (1 in total):
      GE1/0/3                                  (00:01:23)
```

1.15 MLD Snooping常见故障处理

1.15.1 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** 命令开启设备的 MLD Snooping 特性，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。

1.15.2 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；
- 没有开启丢弃未知 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** 命令查看是否已开启丢弃未知 IPv6 组播数据报文的功能。如果没有开启，则使用 **mld-snooping drop-unknown** 命令开启丢弃未知 IPv6 组播数据报文功能。

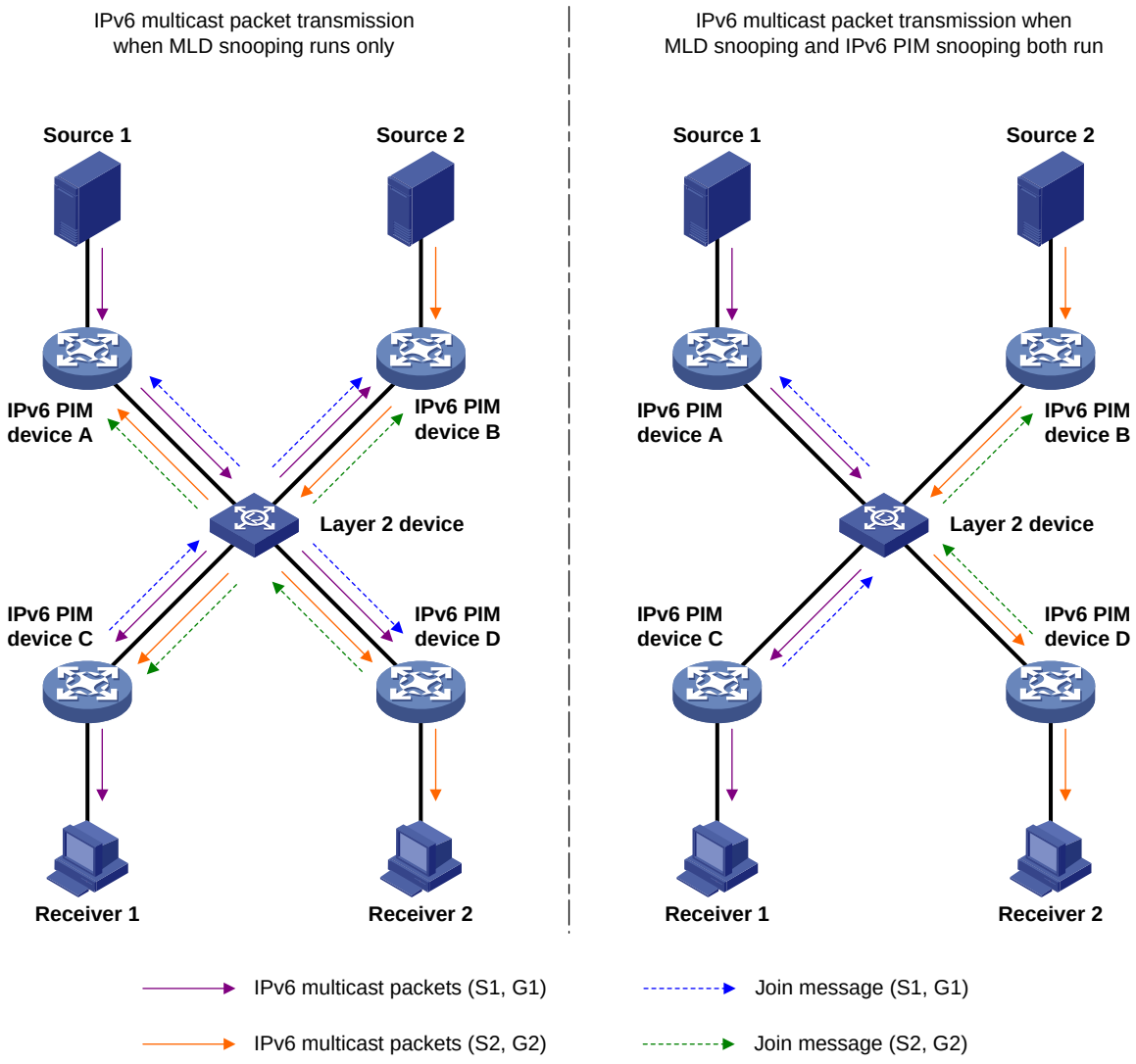
目 录

1 IPv6 PIM Snooping

1.1 IPv6 PIM Snooping简介

IPv6 PIM Snooping（IPv6 Protocol Independent Multicast Snooping，IPv6 协议无关组播窥探）运行在二层设备上，通过与 MLD Snooping 配合来对收到的 IPv6 PIM 协议报文进行分析，将有接收需求的端口添加到 IPv6 PIM Snooping 路由表的相应表项中，以实现 IPv6 组播报文的精确转发。

图1-1 二层设备运行 IPv6 PIM Snooping 前后的对比



如 图 1-1 所示，IPv6 组播源Source 1 和Source 2 分别向IPv6 组播组G1 和G2 发送IPv6 组播数据，而Receiver 1 和Receiver 2 则分别是G1 和G2 的接收者，二层设备上连接各IPv6 PIM路由器的端口都属于同一个VLAN：

- 当二层设备只运行 MLD Snooping 时，它通过监听 IPv6 PIM 路由器发出的 IPv6 PIM Hello 报文来维护路由器端口，将 IPv6 组播数据报文向 VLAN 内的所有路由器端口转发，而将除 IPv6

PIM Hello 报文外的其它 IPv6 PIM 协议报文在 VLAN 内广播。因此，无论 IPv6 PIM 路由器是否有接收需求，都会收到所有的 IPv6 PIM 协议报文和 IPv6 组播数据报文。

- 当二层设备同时运行了 MLD Snooping 和 IPv6 PIM Snooping 时，它通过监听 IPv6 PIM 路由器发出的 IPv6 PIM 协议报文来了解其接收需求，将有接收需求的 IPv6 PIM 路由器所在的端口添加到 IPv6 PIM Snooping 路由表的相应表项中，使 IPv6 PIM 协议报文和 IPv6 组播数据报文能够被精确转发给有接收需求的 IPv6 PIM 路由器，从而节约了网络带宽。

说明

有关 MLD Snooping 和路由器端口的详细介绍，请参见“IP 组播配置指导”中的“MLD Snooping”。

1.2 IPv6 PIM Snooping配置限制和指导

IPv6 PIM Snooping 功能在 Secondary VLAN 中不会生效，因此不建议在 Secondary VLAN 中配置此功能。有关 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“Private VLAN”。

在 VLAN 内使能了 IPv6 PIM Snooping 之后，IPv6 PIM Snooping 功能只在属于该 VLAN 的端口上生效。

1.3 IPv6 PIM Snooping配置任务简介

IPv6 PIM Snooping 配置任务如下：

(1) 使能IPv6 PIM Snooping

(2) （可选）配置主从倒换后IPv6 PIM Snooping全局端口的老化时间

- 配置全局邻居端口的老化时间
- 配置全局下游端口和全局路由器端口的老化时间

1.4 使能IPv6 PIM Snooping

(1) 进入系统视图。

system-view

(2) 开启设备的 MLD Snooping，并进入 MLD-Snooping 视图。

mld-snooping

缺省情况下，MLD Snooping 处于关闭状态。

本命令的详细介绍，请参见“IP 组播命令参考”中的“MLD Snooping”。

(3) 退回系统视图。

quit

(4) 进入 VLAN 视图。

vlan *vlan-id*

(5) VLAN 内使能 MLD Snooping。

mld-snooping enable

缺省情况下，VLAN 内的 MLD Snooping 处于关闭状态。

本命令的详细介绍，请参见“IP 组播命令参考”中的“MLD Snooping”。

(6) VLAN 内使能 IPv6 PIM Snooping。

ipv6 pim-snooping enable

缺省情况下，VLAN 内的 IPv6 PIM Snooping 处于关闭状态。

1.5 配置主从倒换后IPv6 PIM Snooping全局端口的老化时间

1.5.1 功能简介

全局端口指的是主设备的虚拟端口，包括二层聚合接口等。由全局端口担任的邻居端口、下游端口和路由器端口分别称为全局邻居端口、全局下游端口和全局路由器端口。

为了使 IPv6 PIM Snooping 在主从倒换后不会因表项老化而影响二层数据转发，可以手动配置倒换后的全局端口老化时间。

1.5.2 配置限制和指导

当主从倒换后的全局邻居端口收到 IPv6 PIM Hello 报文时，手动配置的全局邻居端口的老化时间将失效，以 IPv6 PIM Hello 报文里的老化时间为准。

当主从倒换后的全局路由器端口和全局下游端口收到 IPv6 PIM 加入报文时，手动配置的全局路由器端口和全局下游端口的老化时间将失效，以 IPv6 PIM 加入报文里的老化时间为准。

1.5.1 配置全局邻居端口的老化时间

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 配置主从倒换后 IPv6 PIM Snooping 全局邻居端口的老化时间。

ipv6 pim-snooping graceful-restart neighbor-aging-time *seconds*

缺省情况下，主从倒换后 IPv6 PIM Snooping 全局邻居端口老化时间为 105 秒。

1.5.2 配置全局下游端口和全局路由器端口的老化时间

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 配置主从倒换后 IPv6 PIM Snooping 全局下游端口和全局路由器端口的老化时间。

ipv6 pim-snooping graceful-restart join-aging-time *seconds*

缺省情况下，主从倒换后 IPv6 PIM Snooping 全局下游端口和全局路由器端口的老化时间为 210 秒。

1.6 IPv6 PIM 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 IPv6 PIM 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 PIM Snooping 的统计信息。

表1-1 IPv6 PIM Snooping 显示和维护

操作	命令
显示IPv6 PIM Snooping的邻居信息	**display ipv6 pim-snooping neighbor** [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]
显示IPv6 PIM Snooping的路由器端口信息	**display ipv6 pim-snooping router-port** [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]
显示IPv6 PIM Snooping路由表的信息	**display ipv6 pim-snooping routing-table** [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]
显示IPv6 PIM Snooping监听到的PIM报文的统计信息	**display ipv6 pim-snooping statistics**
清除IPv6 PIM Snooping监听到的PIM报文的统计信息	**reset ipv6 pim-snooping statistics**

1.7 IPv6 PIM Snooping典型配置举例

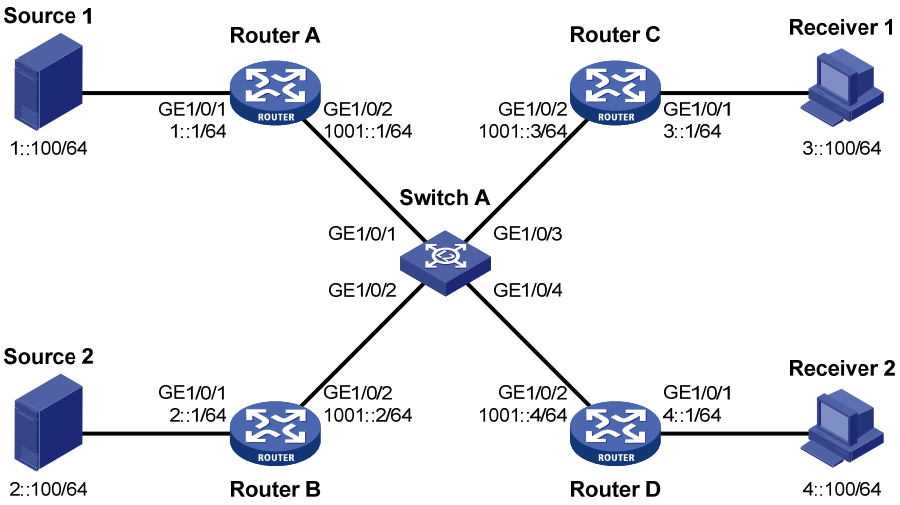
1.7.1 IPv6 PIM Snooping基本组网配置举例

1. 组网需求

- 如 图 1-2 所示，网络中运行OSPFv3 协议，Router A和Router B各自的GigabitEthernet1/0/1 接口分别连接IPv6 组播源Source 1 和Source 2；Router C和Router D各自的 GigabitEthernet1/0/1 接口分别连接接收者Receiver 1 和Receiver 2；Router A、Router B、Router C和Router D各自的GigabitEthernet1/0/2 接口都通过Switch A互连。
- Source 1 和 Source 2 分别通过 IPv6 组播组 FF1E::101 和 FF2E::101 发送 IPv6 组播数据，Receiver 1 和 Receiver 2 则分别接收来自 IPv6 组播组 FF1E::101 和 FF2E::101 的 IPv6 组播数据；Router C 和 Router D 各自的 GigabitEthernet1/0/1 接口上都运行 MLD，Router A、Router B、Router C 和 Router D 上都运行 IPv6 PIM-SM，并由 Router A 的 GigabitEthernet1/0/2 接口充当 C-BSR 和 C-RP。
- 通过在 Switch A 上配置 MLD Snooping 和 IPv6 PIM Snooping，使 Switch A 将 IPv6 PIM 协议报文和 IPv6 组播数据报文只转发给有接收需求的路由器。
- 在所有与 Switch A 相连的 IPv6 PIM 设备上配置加入/剪枝报文的最大长度为 1400 字节，小于 IPv6 路径 MTU。

2. 组网图

图1-2 IPv6 PIM Snooping 典型配置组网图



3. 配置步骤

(1) 配置 IPv6 地址和 IPv6 单播路由协议

请按照 图 1-2 配置各接口的IPv6 地址和前缀长度，并在各路由器上配置OSPFv3 协议，具体配置过程略。

(2) 配置 Router A

使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-SM，设置加入/剪枝报文的最大长度，并配置 C-BSR 和 C-RP。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ipv6 pim sm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ipv6 pim sm
[RouterA-GigabitEthernet1/0/2] quit
[RouterA] ipv6 pim
[RouterA-pim6] jp-pkt-size 1400
[RouterA-pim6] c-bsr 1001::1
[RouterA-pim6] c-rp 1001::1
[RouterA-pim6] quit
```

(3) 配置 Router B

使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-SM，并设置加入/剪枝报文的最大长度。

```
<RouterB> system-view
[RouterB] ipv6 multicast routing
[RouterB-mrib6] quit
[RouterB] interface gigabitethernet 1/0/1
```

```
[RouterB-GigabitEthernet1/0/1] ipv6 pim sm
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] ipv6 pim sm
[RouterB-GigabitEthernet1/0/2] quit
[RouterB] ipv6 pim
[RouterB-pim6] jp-pkt-size 1400
```

(4) 配置 Router C

使能 IPv6 组播路由，在接口 GigabitEthernet1/0/2 上使能 IPv6 PIM-SM，在接口 GigabitEthernet1/0/1 上使能 MLD，并设置加入/剪枝报文的最大长度。

```
<RouterC> system-view
[RouterC] ipv6 multicast routing
[RouterC-mrib6] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] mld enable
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] ipv6 pim sm
[RouterC-GigabitEthernet1/0/2] quit
[RouterC] ipv6 pim
[RouterC-pim6] jp-pkt-size 1400
```

(5) 配置 Router D

使能 IPv6 组播路由，在接口 GigabitEthernet1/0/2 上使能 IPv6 PIM-SM，在接口 GigabitEthernet1/0/1 上使能 MLD，并设置加入/剪枝报文的最大长度。

```
<RouterD> system-view
[RouterD] ipv6 multicast routing
[RouterD-mrib6] quit
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] mld enable
[RouterD-GigabitEthernet1/0/1] quit
[RouterD] interface gigabitethernet 1/0/2
[RouterD-GigabitEthernet1/0/2] ipv6 pim sm
[RouterD-GigabitEthernet1/0/2] quit
[RouterD] ipv6 pim
[RouterD-pim6] jp-pkt-size 1400
```

(6) 配置 Switch A

开启设备的 MLD Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 添加到该 VLAN 中，并在该 VLAN 内使能 MLD Snooping 和 IPv6 PIM Snooping。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] ipv6 pim-snooping enable
```

```
    [SwitchA-vlan100] quit
```

4. 验证配置

显示 Switch A 上 VLAN 100 内 IPv6 PIM Snooping 的邻居信息。

```
[SwitchA] display ipv6 pim-snooping neighbor vlan 100
Total 4 neighbors.

VLAN 100: Total 4 neighbors.
  FE80::1
    Ports (1 in total):
      GE1/0/1                 (00:32:43)
  FE80::2
    Ports (1 in total):
      GE1/0/2                 (00:32:43)
  FE80::3
    Ports (1 in total):
      GE1/0/3                 (00:32:43)
  FE80::4
    Ports (1 in total):
      GE1/0/4                 (00:32:43)
```

由此可见，Router A、Router B、Router C 和 Router D 之间都建立起了 IPv6 PIM Snooping 邻居关系。

显示 Switch A 上 VLAN 100 内 IPv6 PIM Snooping 路由表的信息。

```
[SwitchA] display ipv6 pim-snooping routing-table vlan 100
Total 2 entries.
FSM flag: NI-no info, J-join, PP-prune pending

VLAN 100: Total 2 entries.
  (*, FF1E::101)
    Upstream neighbor: FE80::1
      Upstream ports (1 in total):
        GE1/0/1
      Downstream ports (1 in total):
        GE1/0/3
          Expires: 00:03:01, FSM: J
  (*, FF2E::101)
    Upstream neighbor: FE80::2
      Upstream ports (1 in total):
        GE1/0/2
      Downstream ports (1 in total):
        GE1/0/4
          Expires: 00:03:01, FSM: J
```

由此可见，Switch A 将向 Router C 转发 IPv6 组播组 FF1E::101 的 IPv6 组播数据，向 Router D 转发 IPv6 组播组 FF2E::101 的 IPv6 组播数据。

1.8 IPv6 PIM Snooping常见故障处理

1.8.1 二层设备不能实现IPv6 PIM Snooping功能

1. 故障现象

二层设备不能实现 IPv6 PIM Snooping 功能。

2. 故障分析

MLD Snooping 或 IPv6 PIM Snooping 没有使能。

3. 处理过程

(1) 使用 **display current-configuration** 命令查看 MLD Snooping 和 IPv6 PIM Snooping 的运行状态。

(2) 如果没有使能 MLD Snooping，请先开启设备的 MLD Snooping，然后分别使能 VLAN 内的 MLD Snooping 和 IPv6 PIM Snooping。

(3) 如果没有使能 IPv6 PIM Snooping，请使能 VLAN 内的 IPv6 PIM Snooping。

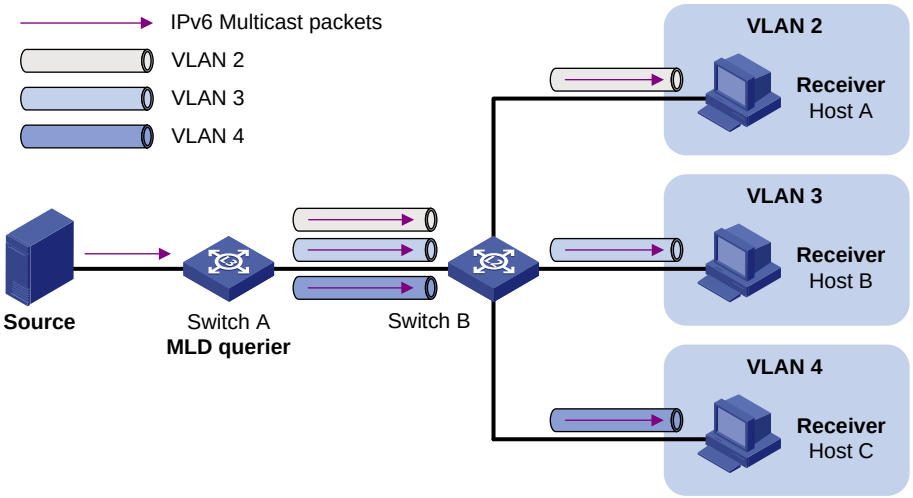
目 录

1 IPv6 组播VLAN

1.1 IPv6组播VLAN作用

如 图 1-1 所示，在传统的IPv6 组播点播方式下，当属于不同VLAN的主机Host A、Host B和Host C同时点播同一IPv6 组播组时，三层设备（Switch A）需要将IPv6 组播数据为每个用户VLAN（即主机所属的VLAN）都复制一份后发送给二层设备（Switch B）。这样既造成了带宽的浪费，也给三层设备增加了额外的负担。

图1-1 未运行 IPv6 组播 VLAN 时的 IPv6 组播数据传输



可以使用 IPv6 组播 VLAN 功能解决这个问题。在二层设备上配置了 IPv6 组播 VLAN 后，三层设备只需将 IPv6 组播数据通过 IPv6 组播 VLAN 向二层设备发送一份即可，而不必为每个用户 VLAN 都复制一份，从而节省了网络带宽，也减轻了三层设备的负担。

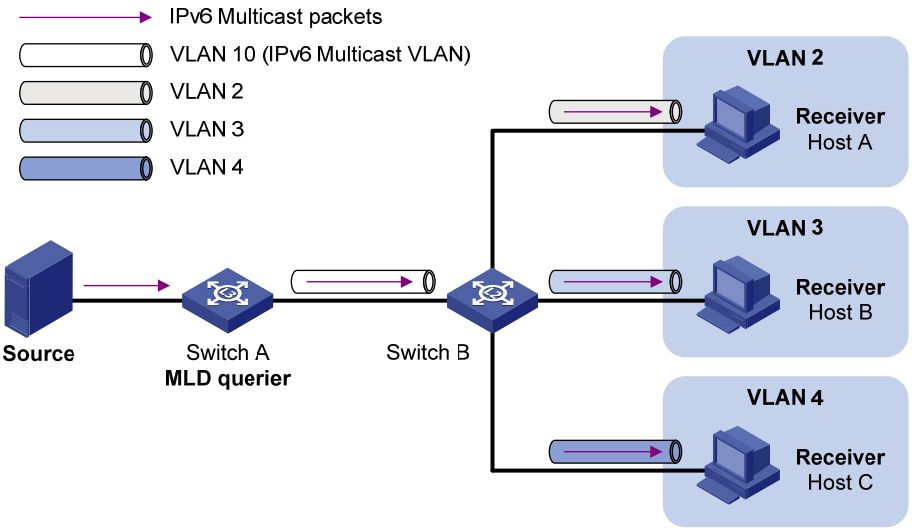
1.2 IPv6组播VLAN实现方式

IPv6 组播 VLAN 有基于子 VLAN 和基于端口两种实现和配置方式。

1.2.1 基于子VLAN的IPv6 组播VLAN

如 图 1-2 所示，接收者主机Host A、Host B和Host C分属不同的用户VLAN。在Switch B上配置VLAN 10 为IPv6 组播VLAN，将所有的用户VLAN都配置为该IPv6 组播VLAN的子VLAN，并在IPv6 组播VLAN及其子VLAN内都使能MLD Snooping。

图1-2 基于子 VLAN 的 IPv6 组播 VLAN 示意图

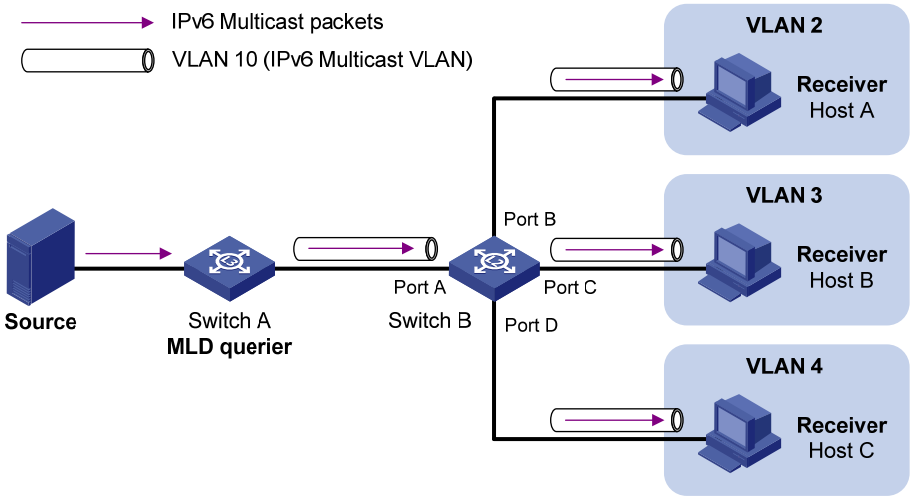


配置完成后，MLD Snooping 将在 IPv6 组播 VLAN 中对路由器端口进行维护，而在各子 VLAN 中对成员端口进行维护。这样，Switch A 只需将 IPv6 组播数据通过 IPv6 组播 VLAN 向 Switch B 发送一份即可，Switch B 会将其复制分发给该 IPv6 组播 VLAN 内那些有接收者的子 VLAN。

1.2.2 基于端口的IPv6 组播VLAN

如 图 1-3 所示，接收者主机Host A、Host B和Host C分属不同的用户VLAN，Switch B上的所有用户端口（即连接主机的端口）均为Hybrid类型。在Switch A上配置VLAN 10 为IPv6 组播VLAN，将所有用户端口都添加到该IPv6 组播VLAN内，并在IPv6 组播VLAN和所有用户VLAN内都使能MLD Snooping。

图1-3 基于端口的 IPv6 组播 VLAN 示意图



配置完成后，当 Switch B 上的用户端口收到来自主机的 MLD 报文时，会为其打上 IPv6 组播 VLAN 的 Tag 并上送给 MLD 查询器，于是 MLD Snooping 就可以在 IPv6 组播 VLAN 中对路由器端口和成

员端口进行统一的维护。这样，Switch A 只需将 IPv6 组播数据通过 IPv6 组播 VLAN 向 Switch B 发送一份即可，Switch B 会将其复制分发给该 IPv6 组播 VLAN 内的所有成员端口。

1.3 IPv6组播VLAN配置限制和指导

要配置为 IPv6 组播 VLAN 的指定 VLAN 必须存在。

若在设备上同时配置了基于子 VLAN 和基于端口的 IPv6 组播 VLAN，则基于端口的 IPv6 组播 VLAN 将优先生效。

IPv6 组播 VLAN 功能在 Secondary VLAN 中不会生效，因此不建议在 Secondary VLAN 中配置此功能。有关 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“Private VLAN”。

1.4 配置基于子VLAN的IPv6组播VLAN

1. 配置限制和指导

要添加到 IPv6 组播 VLAN 内的子 VLAN 必须存在，且不能是 IPv6 组播 VLAN 或其它 IPv6 组播 VLAN 的子 VLAN。

2. 配置准备

在配置基于子 VLAN 的 IPv6 组播 VLAN 之前，需完成以下任务：

- 创建相应的 VLAN
- 在欲配置为 IPv6 组播 VLAN 及其子 VLAN 的所有 VLAN 内使能 MLD Snooping

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置指定 VLAN 为 IPv6 组播 VLAN，并进入 IPv6 组播 VLAN 视图。

ipv6 multicast-vlan *vlan-id*

缺省情况下，VLAN 不是 IPv6 组播 VLAN。

(3) 向 IPv6 组播 VLAN 内添加子 VLAN。

subvlan *vlan-list*

1.5 配置基于端口的IPv6组播VLAN

1. 配置限制和指导

既可以在 IPv6 组播 VLAN 内添加端口，也可以在端口上指定其所属的 IPv6 组播 VLAN——这两种配置方式是等效的。

一个端口只能属于一个 IPv6 组播 VLAN。

2. 配置准备

在配置基于端口的 IPv6 组播 VLAN 之前，需完成以下任务：

- 创建相应的 VLAN
- 在欲配置为 IPv6 组播 VLAN 的 VLAN 内使能 MLD Snooping

- 在所有的用户 VLAN 内都使能 MLD Snooping
- 配置用户端口属性，保证当二层设备通过 IPv6 组播 VLAN 收到来自上游、打有 IPv6 组播 VLAN Tag 的 IPv6 组播数据报文时，会将其 Tag 去掉后再向下游转发。有关配置用户端口属性的详细介绍，请参见“二层技术-以太网交换命令参考”中的“VLAN”。

3. 在IPv6 组播VLAN内配置IPv6 组播VLAN端口

(1) 进入系统视图。

system-view

(2) 配置指定 VLAN 为 IPv6 组播 VLAN，并进入 IPv6 组播 VLAN 视图。

ipv6 multicast-vlan *vlan-id*

缺省情况下，VLAN 不是 IPv6 组播 VLAN。

(3) 向 IPv6 组播 VLAN 内添加端口。

port *interface-list*

4. 在端口上配置IPv6 组播VLAN端口

(1) 进入系统视图。

system-view

(2) 配置指定 VLAN 为 IPv6 组播 VLAN，并进入 IPv6 组播 VLAN 视图。

ipv6 multicast-vlan *vlan-id*

缺省情况下，VLAN 不是 IPv6 组播 VLAN。

(3) 退回系统视图。

quit

(4) 进入二层接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(5) 指定端口所属的 IPv6 组播 VLAN。

ipv6 port multicast-vlan *vlan-id*

缺省情况下，端口不属于任何 IPv6 组播 VLAN。

1.6 配置IPv6组播VLAN转发表项的最大数量

1. 功能简介

用户可以调整 IPv6 组播 VLAN 转发表项的最大数量，当所有 IPv6 组播 VLAN 内维护的表项总数达到最大数量后，将不再创建新的表项，直至有表项被老化或被手工删除。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 IPv6 组播 VLAN 转发表项的最大数量。

ipv6 multicast-vlan entry-limit *limit*

缺省情况下，组播 VLAN 转发表项的最大数量为 250。

1.7 IPv6组播VLAN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 IPv6 组播 VLAN 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 VLAN 的统计信息。

表1-1 IPv6 组播 VLAN 显示和维护

操作	命令
显示IPv6组播VLAN的信息	**display ipv6 multicast-vlan** [*vlan-id*]
显示IPv6组播VLAN转发表的信息	**display ipv6 multicast-vlan forwarding-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **slot** *slot-number* | **subvlan** *vlan-id* | **vlan** *vlan-id*] *
显示IPv6组播VLAN的组播组表项信息	**display ipv6 multicast-vlan group** [*ipv6-source-address* | *ipv6-group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *
清除IPv6组播VLAN的组播组表项	**reset ipv6 multicast-vlan group** [*ipv6-group-address* [*prefix-length*] | *ipv6-source-address* [*prefix-length*] | **vlan** *vlan-id*] *

1.8 IPv6组播VLAN典型配置举例

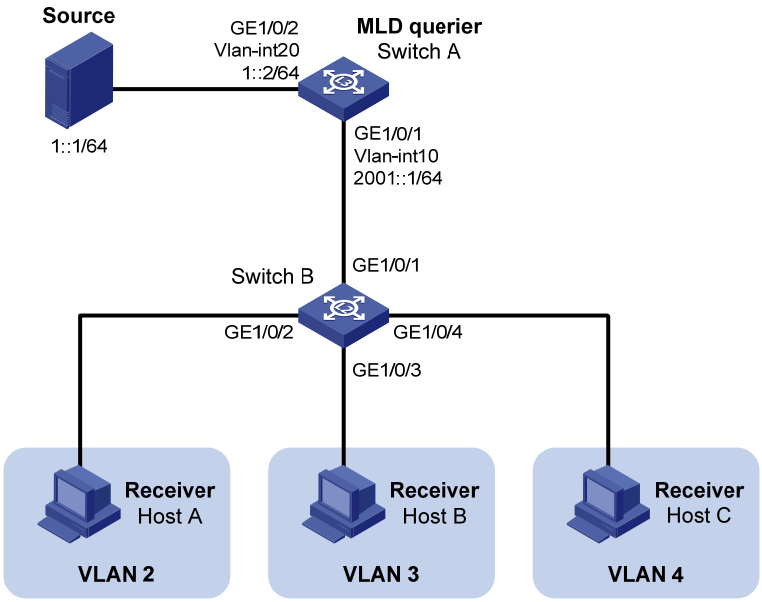
1.8.1 基于子VLAN的IPv6 组播VLAN配置举例

1. 组网需求

- 如 图 1-4 所示，三层交换机Switch A通过接口VLAN-interface20 连接IPv6 组播源（Source），通过接口VLAN-interface10 连接二层交换机Switch B；Switch A上运行MLDv1，Switch B上运行版本 1 的MLD Snooping，并由Switch A充当MLD查询器。
- IPv6 组播源向 IPv6 组播组 FF1E::101 发送 IPv6 组播数据，Host A～Host C 都是该 IPv6 组播组的接收者（Receiver），且分别属于 VLAN 2～VLAN 4。
- 通过在 Switch B 上配置基于子 VLAN 的 IPv6 组播 VLAN，Switch A 通过 IPv6 组播 VLAN 向 Switch B 下分属不同用户 VLAN 的主机分发 IPv6 组播数据。

2. 组网图

图1-4 基于子 VLAN 的 IPv6 组播 VLAN 配置组网图



3. 配置步骤

(1) 配置 Switch A

使能 IPv6 组播路由。

```
<SwitchA> system-view
[SwitchA] ipv6 multicast routing
[SwitchA-mrib6] quit
```

创建 VLAN 20，并将端口 GigabitEthernet1/0/2 加入该 VLAN。

```
[SwitchA] vlan 20
[SwitchA-vlan20] port gigabitethernet 1/0/2
[SwitchA-vlan20] quit
```

在接口 VLAN-interface20 上配置 IPv6 地址，并使能 IPv6 PIM-DM。

```
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ipv6 address 1::2 64
[SwitchA-Vlan-interface20] ipv6 pim dm
[SwitchA-Vlan-interface20] quit
```

创建 VLAN 10，配置端口 GigabitEthernet1/0/1 为 Hybrid 端口，并允许 VLAN 10 的报文带 Tag 通过。

```
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type hybrid
[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 10 tagged
[SwitchA-GigabitEthernet1/0/1] quit
```

在接口 VLAN-interface10 上配置 IPv6 地址，并使能 MLD。

```
[SwitchA] interface vlan-interface 10
```

```
[SwitchA-Vlan-interface10] ipv6 address 2001::1 64
[SwitchA-Vlan-interface10] mld enable
[SwitchA-Vlan-interface10] quit
```

(2) 配置 Switch B

开启设备的 MLD Snooping。

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

创建 VLAN 2，将端口 GigabitEthernet1/0/2 加入该 VLAN，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/2
[SwitchB-vlan2] mld-snooping enable
[SwitchB-vlan2] quit
```

创建 VLAN 3，将端口 GigabitEthernet1/0/3 加入该 VLAN，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/3
[SwitchB-vlan3] mld-snooping enable
[SwitchB-vlan3] quit
```

创建 VLAN 4，将端口 GigabitEthernet1/0/4 加入该 VLAN，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchB] vlan 4
[SwitchB-vlan4] port gigabitethernet 1/0/4
[SwitchB-vlan4] mld-snooping enable
[SwitchB-vlan4] quit
```

创建 VLAN 10，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchB] vlan 10
[SwitchB-vlan10] mld-snooping enable
[SwitchB-vlan10] quit
```

配置端口 GigabitEthernet1/0/1 为 Hybrid 端口，并允许 VLAN 10 的报文带 Tag 通过。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type hybrid
[SwitchB-GigabitEthernet1/0/1] port hybrid vlan 10 tagged
[SwitchB-GigabitEthernet1/0/1] quit
```

配置 VLAN 10 为 IPv6 组播 VLAN，并把 VLAN 2～VLAN 4 都配置为该 IPv6 组播 VLAN 的子 VLAN。

```
[SwitchB] ipv6 multicast-vlan 10
[SwitchB-ipv6-mvlan-10] subvlan 2 to 4
[SwitchB-ipv6-mvlan-10] quit
```

4. 验证配置

显示 Switch B 上所有 IPv6 组播 VLAN 的信息。

```
[SwitchB] display ipv6 multicast-vlan
Total 1 IPv6 multicast VLANs.
```

```
IPv6 multicast VLAN 10:
  Sub-VLAN list(3 in total):
     2-4
  Port list(0 in total):
```

显示 Switch B 上 IPv6 组播 VLAN 的所有组播组表项信息。

```
[SwitchB] display ipv6 multicast-vlan group
Total 1 entries.

IPv6 multicast VLAN 10: Total 1 entries.
  (::, FF1E::101)
    Sub-VLANs (3 in total):
      VLAN 2
      VLAN 3
      VLAN 4
```

由此可见，IPv6 组播 VLAN（VLAN 10）在各子 VLAN（VLAN 2～VLAN 4）内维护组播组表项。

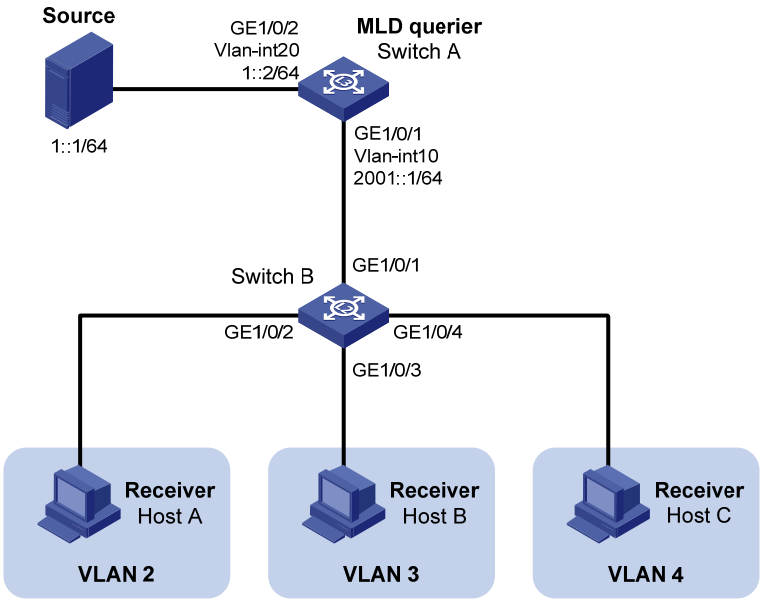
1.8.2 基于端口的IPv6 组播VLAN配置举例

1. 组网需求

- 如 图 1-5 所示，三层交换机Switch A通过接口VLAN-interface20 连接IPv6 组播源（Source），通过接口VLAN-interface10 连接二层交换机Switch B；Switch A上运行MLDv1，Switch B上运行版本 1 的MLD Snooping，并由Switch A充当MLD查询器。
- IPv6 组播源向 IPv6 组播组 FF1E::101 发送 IPv6 组播数据，Host A～Host C 都是该 IPv6 组播组的接收者（Receiver），且分别属于 VLAN 2～VLAN 4。
- 通过在 Switch B 上配置基于端口的 IPv6 组播 VLAN，使 Switch A 通过 IPv6 组播 VLAN 向 Switch B 下分属不同用户 VLAN 的主机分发 IPv6 组播数据。

2. 组网图

图1-5 基于端口的 IPv6 组播 VLAN 配置组网图



3. 配置步骤

(1) 配置 Switch A

使能 IPv6 组播路由。

```
<SwitchA> system-view
[SwitchA] ipv6 multicast routing
[SwitchA-mrib6] quit
```

创建 VLAN 20，并将端口 GigabitEthernet1/0/2 加入该 VLAN。

```
[SwitchA] vlan 20
[SwitchA-vlan20] port gigabitethernet 1/0/2
[SwitchA-vlan20] quit
```

在接口 VLAN-interface20 上配置 IPv6 地址，并使能 IPv6 PIM-DM。

```
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ipv6 address 1::2 64
[SwitchA-Vlan-interface20] ipv6 pim dm
[SwitchA-Vlan-interface20] quit
```

创建 VLAN 10，将端口 GigabitEthernet1/0/1 加入该 VLAN。

```
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/1
[SwitchA-vlan10] quit
```

在接口 VLAN-interface10 上配置 IPv6 地址，并使能 MLD。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ipv6 address 2001::1 64
[SwitchA-Vlan-interface10] mld enable
[SwitchA-Vlan-interface10] quit
```

(2) 配置 Switch B

开启设备的 MLD Snooping。

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

创建 VLAN 10，把端口 GigabitEthernet1/0/1 加入该 VLAN，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchB] vlan 10
[SwitchB-vlan10] port gigabitethernet 1/0/1
[SwitchB-vlan10] mld-snooping enable
[SwitchB-vlan10] quit
```

创建 VLAN 2，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchB] vlan 2
[SwitchB-vlan2] mld-snooping enable
[SwitchB-vlan2] quit
```

创建 VLAN 3，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchB] vlan 3
[SwitchB-vlan3] mld-snooping enable
[SwitchB-vlan3] quit
```

创建 VLAN 4，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchB] vlan 4
[SwitchB-vlan4] mld-snooping enable
[SwitchB-vlan4] quit
```

配置端口 GigabitEthernet1/0/2 为 Hybrid 类型，缺省 VLAN 为 VLAN 2；允许 VLAN 2 和 VLAN 10 的报文不带 Tag 通过。

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type hybrid
[SwitchB-GigabitEthernet1/0/2] port hybrid pvid vlan 2
[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 2 untagged
[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/2] quit
```

配置端口 GigabitEthernet1/0/3 为 Hybrid 类型，缺省 VLAN 为 VLAN 3；允许 VLAN 3 和 VLAN 10 的报文不带 Tag 通过。

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-type hybrid
[SwitchB-GigabitEthernet1/0/3] port hybrid pvid vlan 3
[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 3 untagged
[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/3] quit
```

配置端口 GigabitEthernet1/0/4 为 Hybrid 类型，缺省 VLAN 为 VLAN 4；允许 VLAN 4 和 VLAN 10 的报文不带 Tag 通过。

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] port link-type hybrid
[SwitchB-GigabitEthernet1/0/4] port hybrid pvid vlan 4
[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 4 untagged
[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/4] quit
```

配置 VLAN 10 为 IPv6 组播 VLAN。

```
[SwitchB] ipv6 multicast-vlan 10
```

将端口 GigabitEthernet1/0/2 到 GigabitEthernet1/0/3 加入 IPv6 组播 VLAN 10。

```
[SwitchB-ipv6-mvlan-10] port gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[SwitchB-ipv6-mvlan-10] quit
```

配置端口 GigabitEthernet1/0/4 也属于 IPv6 组播 VLAN 10。

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] ipv6 port multicast-vlan 10
[SwitchB-GigabitEthernet1/0/4] quit
```

4. 验证配置

显示 Switch B 上所有 IPv6 组播 VLAN 的信息。

```
[SwitchB] display ipv6 multicast-vlan
Total 1 IPv6 multicast VLANs.

IPv6 multicast VLAN 10:
  Sub-VLAN list(0 in total):
  Port list(3 in total):
    GE1/0/2
    GE1/0/3
    GE1/0/4
```

显示 Switch B 上 IPv6 动态组播组的 MLD Snooping 转发表项信息。

```
[SwitchB] display mld-snooping group
Total 1 entries.

VLAN 10: Total 1 entries.
  (::, FF1E::101)
    Host slots (0 in total):
    Host ports (3 in total):
      GE1/0/2        (00:03:23)
      GE1/0/3        (00:04:07)
      GE1/0/4        (00:04:16)
```

由此可见，MLD Snooping 统一在 IPv6 组播 VLAN（VLAN 10）中维护成员端口。