银河风云
nROSE 配置手册
IP 组播分册

文档编号：0205_S5300_v5.2_100706

深圳市银河风云网络系统股份有限公司

地址：深圳市科技园北区松坪新西路五号风云大厦

邮编：518057

电话：（0755）83400088

传真：（0755）33630995

客服：800-999-8305

网址：http://www.galaxywind.com

邮箱：customer@galaxywind.com

目录

第1章 IP 组播

1.1. IP 组播简介

当代社会已经进入信息时代，网络技术在飞速发展。由于视频会议、推送技术、大规模协作计算、为用户群进行软件升级、用于培训和企业报告的共享白板式的多媒体应用、网络代理、镜像和高速缓存站点等等应用，都依赖于从一个主机向多个主机或者从多个主机向多个主机发送同一信息的能力，而在 Internet 上分发的数目可能达数十万台，这些都需要更高的带宽，并且大大超出了单播的能力。

在传统的单播（Unicast，即为每个用户单独建立一条数据传送通路）的方式下，发送信息的主机必须向每个希望接收此数据包的用户发送一份单独的数据包拷贝。这种巨大的冗余会带来很大的代价。首先，会给发送数据的源主机带来沉重的负担，因为它必须对每个要求都做出响应，这使得负担过于沉重主机的响应会大大延长。其次对三层交换机和交换机的性能也提出了更高的要求，管理人员被迫购买本来不必要的硬件和带宽来保证一定的服务质量。

在 IP 通信另一个领域是 IP 广播（Broadcast），在这里，源主机向一个网段中的所有 IP 主机发送 IP 信息包，不管他们是否需要，都会接收到广播来的信息，这样便导致了所有机器上的资源消耗。

如在一个网络上有 300 个用户需要接收相同的信息时，传统的解决方案要么把这一信息分别发送 300 次，以便确保每个需要数据的用户都能够得到所需的数据，要么采用广播的方式，在整个网络范围内传送数据，需要这些数据的用户可直接在网络上获取。以上两种方式都浪费了大量宝贵的带宽资源，而且也不利于信息的安全和保密。

解决上述这些 IP 单播和 IP 广播问题的办法是构建一种具有组播能力的网络，允许三层交换机一次将数据包复制到多个通道上。

IP 组播是一项旨在节省带宽的技术，通过向数千个用户同步传送一个单独的数据流降低网络流量。采用组播方式，单台服务器能够对几十万台主机同时发送连续数据流而无延时。组播发送方只要发送一个信息包而不是很多个，所有目的地同时收到同一信息包，更及时，更同步，可以把信息发送到任意不知名目的地，能减少网络上传输的信息包的总量。

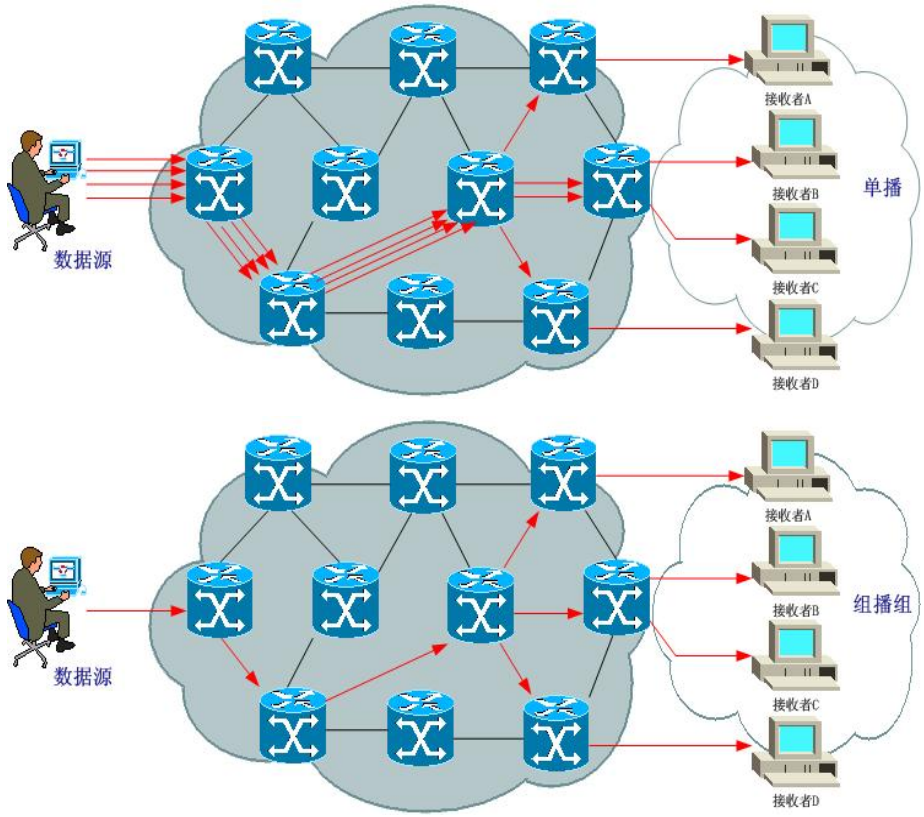


图 1–1 单播与组播传送消息的对比示意图

从图 1-1 可以清楚的看出，单播传送发送数据的多个拷贝，每个拷贝发送到一个接收者，主机轮流发送数据的拷贝，网络分别将它们转发至每个接收者，主机一次只能发送至一个接收者。而组播传送则只把发送数据的一个拷贝发送到多个接收者，主机发送数据的一个拷贝，可同时发送到多个接收者。网络在每个接收者的最后一个三层交换机或主机复制它，在一个给定的网络上每一个包只传送一次。所以，组播技术不但大大节省了带宽资源，还减轻了源端及中间三层交换机节点处理重复分组的负担，缩短了通信所需的处理时间，大大提高了网络处理效率。

1.1.1.IP 组播特性

在 IP 组播环境中，所有的信息接收者都加入到对应的组播组内。信息接收者加入组播组后，流向组地址的数据立即开始传输给接收者，组中的所有成员都能接收到数据。因此为了接收数据，信息接收者必须首先成为组播组的成员。组播环境中，数据传向组中的所有成员，非组内成员不会收到这些数据。

IP 组播具有下列特性：

- 对组成员的数量和所处位置没有限制。独立的主机可以在任意时刻自由地加入或离开组播组。一台主机在同一时刻可以是多个组播组的成员。
- 用户的增加和去除不需要全局协调，加入组播组仅是需要为用户设置一个 IP 组播地址。为了接收数据，用户在特殊 IP 组播交叉点中进行注册，而不需要知道组中其它用户的情况，路由对用户隐藏了组播实现的细节。
- 如果组播起源于同一个源，而终止不同的用户，且携带的数据相同，需要定义一个组播地址，让网络决定如何将源数据流发往组播地址，如何在它的链路上组织数据流传输，以最佳地利用带宽。
- 三层交换机建立分布树，用于连接组播组所有成员，把那些寻址到组播组的 IP 分组一直转发到具有组播组成员的网络中，并解决组播路由选择中的回路问题。
- 发送者使用组播地址发送分组，发送方可以不知道接收方的任何信息，而只需要了解地址。一个组可有任何源。
- 即使网络中的一台主机不是某个组播组的成员，该主机也可向这个组播组发送数据。

1.1.2.IP 组播地址

IP 组播地址，或称为主机组地址，由 D 类 IP 地址标记。D 类 IP 地址的最高四位为“1110”，起始范围从 224.0.0.0 到 239.255.255.255。如前所述，部分 D 类地址被保留，用作永久组的地址，这段地址从 224.0.0.0-224.0.0.255。临时主机组的组播地址由网络管理员选择，他需要保证这个地址在一定的范围内没有其他的主机组在使用这个组播地址。

D 类地址范围与含义可如下表所示：

表 1–1 D 类地址的范围及含义

D 类地址范围	含义
224.0.0.0~224.0.0.255	预留的组播地址（永久组地址）
224.0.1.0~238.255.255.255	用户可用的组播地址（临时组地址）
239.0.0.0~239.255.255.255	本地被管理的或特定位置的组播地址

常用的预留组播地址列表如下：

表 1–2 预留的组播地址列表

D 类地址范围	含义
224.0.0.0	基准地址（保留）
224.0.0.1	直连网络上的所有主机的地址
224.0.0.2	子网上所有路由器的地址
224.0.0.3	不分配
224.0.0.4	DVMRP 路由器
224.0.0.5	OSPF 路由器
224.0.0.6	OSPF DR
224.0.0.7	ST 路由器
224.0.0.8	ST 主机
224.0.0.9	RIP-2 路由器
224.0.0.10	IGRP 路由器
224.0.0.11	活动代理
224.0.0.12	DHCP 服务器/中继代理
224.0.0.13	所有 PIM 路由器
224.0.0.14	RSVP 封装
224.0.0.15	所有 CBT 路由器
224.0.0.16	指定 SBM
224.0.0.17	所有 SBMS
224.0.0.18	VRRP

1.1.3.组播 MAC 地址

第 2 层的组播地址（组播 MAC 地址）可以从 IP 组播地址中衍生。计算方法是把 IP 地址的最后 23 位映射到 MAC 地址的最后 23 位（如图 1-2 所示），然后把这 23 位前面的那一位置为 0。IANA（Internet Assigned Number Authority）规定，MAC 地址的前 24 位必须为 0x01-00-5E。例如：组播 IP 地址 224.0.1.128，16 进制表示为 0xE0-00-01-80，最低的 23

位为 0x00-01-80，计算得出的 MAC 地址为：0x01-00-5E-00-01-80。

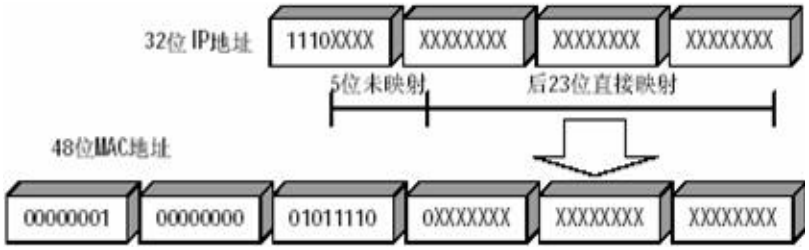


图 1–2 组播 IP 地址与以太网 MAC 地址的映射关系

由于 IP 组播地址的后 28 位中只有 23 位被映射到 MAC 地址，这样就会有 32 个 IP 组播地址映射到同一 MAC 地址上。

1.1.4.IP 组播路由协议

组播路由协议的主要任务就是构造组播的分布树，使组播分组能够传送到相应的组播组成员。组播协议包括两个部分：因特网组管理协议（IGMP）作为 IP 组播基本信令协议；组播路由协议（例如：PIM-SM、PIM-DM）实现 IP 组播流寻径。

1、主机-路由协议

IGMP 协议是一种注册协议，主要完成多播用户组的管理，它定义了主机与三层交换机之间组播成员关系的建立和维护机制，主要完成多播用户组的管理。利用 IGMP 协议，主机与直接连接的三层交换机打交道，通知三层交换机主机希望加入或离开哪一个多播组。多播三层交换机可以判断出在它所直接相连的网段中是否存在多播组的成员。如果存在多播组成员，多播三层交换机就可以向上级多播三层交换机发送消息，申请加入一个多播组，并将上级多播三层交换机发送过来的多播数据包转发给多播成员主机。

2、组播路由协议

因为组播组地址是虚拟的，组播把数据发送给一组希望接收数据的接收者（组播地址），而不是仅仅传送给一个接收者（单播地址）。所以组播不可能如同单播那样，直接从数据源一端路由到特定的目的地址。

组播路由协议的任务就是构建分发树——从数据源端到多个接收端的无环数据传输路径。组播三层交换机能采用多种方法来建立数据传输分发树。根据网络的实际情况，常见的组播路由协议可以分成两大类——密集模式组播路由协议（DM）和稀疏模式

组播路由协议（SM）。

1) 密集模式组播

DM 路由协议通常用于组播成员较为集中、数量较多并且有足够带宽的网路环境，比如公司或园区的局域网。它假设网络中的每个子网有至少一个接收者要接收组播信息。在密集组播模式下，组播报文被扩散到网络中的所有点，与此伴随着网络资源（带宽和三层交换机的 CPU 等）的消耗。

为了减少网络资源的消耗，密集模式组播路由协议对没有组播数据转发的分支进行剪枝操作，只保留包含接收站点的分支。被剪掉的分支中，如果存在接收站点有组播数据转发需求，希望重新接收组播数据流，密集模式组播路由协议可以周期性地将剪掉的分支恢复成转发状态。为了减少将被剪掉的分支恢复成转发状态的等待时间，密集模式组播路由协议使用嫁接机制，将希望恢复成转发状态的被剪掉的分支主动加入组播分布树。这种周期性的扩散和剪枝现象是密集模式协议的特征。一般说来，密集模式下数据的转发路径是一棵“有源树”——以“源”为根、组员为枝叶的树。

DM 模式下典型路由协议有：

- DVMRP：距离向量组播路由协议。这是一种基于距离向量算法的组播路由协议。目前已基本上被 PIM 和 MOSPF 所取代。
- MOSPF：组播 OSPF 协议。
- PIM-DM：协议无关组播协议－密集模式。它不需要单独的组播协议，利用三层交换机上单播路由协议的路由表作反向路径转发检查，由此获得组播分布树。相比另两种协议，PIM-DM 的开销要小很多，它用于组播源和目的非常靠近、接收者数量大于发送者数量并且组播流量比较大的环境中效果很好。

2) 稀疏模式组播

在网路中稀疏分布、网络也没有充足带宽的情况，如广域网环境，可以使用 SM 路由协议。因此，SM 路由协议采用选择性的建立和维护分布树的方式，由空树

开始，仅当成员显式的请求加入分布树才做出修改。稀疏模式组播路由协议周期性地向分支发送加入消息，避免共享树的分支由于没有及时更新而被删除，从而有效地维护共享树。

在稀疏组播模式下，组播数据发送端如果想要给特定的组播组发送数据，首先要在汇聚点进行注册，之后把数据发向汇聚点。当组播数据到达了汇聚点后，数据被复制，然后沿着分发树路径被转发给对其感兴趣的接收者。数据复制仅发生在分发树的分支处，这个过程自动重复，直到报文最终到达目的地。

稀疏模式下的典型路由协议有：

- CBT：基于中心的分布树协议（RFC 2201）。协议由以一个中心的三层交换机为根构造一个共享分布树，所有的组播流量都经由这个中心三层交换机转发。
- PIM-SM：协议无关组播协议－稀疏模式。工作原理与 PIM－DM 类似，但专门针对稀疏环境优化。适用于组播组中接收者较少、间歇性组播流量的情况。不同于 PIM-DM 的泛洪方式，PIM-SM 定义了一个集合点（RP），所有的接收者在 RP 注册，组播分组由 RP 转发给接收者。

1.1.5.IP 组播报文转发

与单播模型不同，组播模型不能将转发决定建立在数据报文中的目标地址基础上，而必须将组播信息报文转发到多个外部接口上以便能传送到所有接收站点，因此组播转发过程比单播转发过程更加复杂。

为了保证组播信息报文都是通过最短路径到达三层交换机，组播模型必须依靠单播路由表或者独立的组播路由表，对组播信息报文的接收接口进行一定的检查，这种检查机制就是大部分组播路由协议进行组播转发的基础——RPF（Reverse Path Forwarding——逆向路径转发）检查。组播应用程序检查到达的组播报文的源地址（如果使用的是有源树，这个源地址就是发送组播报文的源主机的地址；如果使用的是共享树，这个源地址就是共享树的根的地址），以确定此报文到达的入接口处于接收站点至源地址的最短路径上。当组播报文到达三层交换机时，如果检查通过，报文按照组播转发项进行转发，否则，报文被丢弃。

1.1.6.IP 组播应用

1、数据分发

数据分发是 IP 组播应用的一个领域。通过使用 IP 组播，公司可以采用“推”的模式进行文件和数据库更新。这项技术允许公司每天夜里向他们的远程办公室发布新的信息，比如价格和产品信息。企业可使用软件通过卫星链路向所属分公司分发软件升级和数据更新消息。一次性向所有的分公司传送一种数据，而不是依次向每个分公司重发，节省了时间和通信费用。

2、实时数据组播

实时数据传送是使 IP 组播深受欢迎的又一应用领域。一个好的例子是将股票信息发送到交易大厅的工作站。通过指定不同的财务分类（债券、运输、药品等等）给不同的组播组，交易员能使用他们的工作站来接收他们感兴趣的实时金融数据。

IP 组播目前在该领域已获得了一定范围的商业应用。例如企业可在其企业网上使用组播向各个部门分发市场数据。这样做的优点是：如果使用单播系统出现故障时，数据被备份下来，而后当故障排除时，网络上的所有数据存储器开始重发它们备份的数据。这可能再度堵塞网络，从而可能使故障情况再次发生，造成网络停止运行一段时间，然后又再次备份数据。而如果采用组播，这些数据风暴就少多了，因为组播的第一次重发操作是很有效的。

1.2. 组播公共配置

组播公共配置由组播组管理协议和组播路由协议配置共同构成。

1.2.1.使能组播协议

在所有接口上启动组播协议，使三层交换机能转发组播报文。只有使能了组播协议，其它与组播转发有关的配置才能生效。

表 1–3 使能/禁用组播协议

命令	命令模式	功能说明
ip multicast-routing	全局配置模式	使能组播协议。

no ip multicast-routing	全局配置模式	禁用组播协议。

缺省情况下，系统禁用组播协议。

1.2.2.组播监控与维护

完成配置后，可执行 **show** 命令显示配置后组播的运行情况，通过查看显示信息验证配置的效果；执行 **debug** 命令可对组播进行调试。

表 1–4 组播监控与维护

命令	命令模式	功能说明
show ip mroute [**vrf** *vrf-name*] [*group-address* [**source** *source-address*] | **count**]	特权用户模式	显示组播路由表信息。
debug ip mrouting [**vrf** *vrf-name*] [*group-address*]	特权用户模式	打开组播转发表调试信息开关。
debug ip mpacket [**vrf** *vrf-name*] [*group-address* | **list** *list-num*]	特权用户模式	打开组播报文调试信息开关。

【示例】显示组播路由表信息。

```
Tritium# show ip mroute
  IP Multicast Routing Table
  Flags : D - Dense, S - Sparse, C - Connected
          L - Local, P - Pruned, R - RP - bit set, F - Register flag
          T - SPT - bit set, J - Join SPT, N - Injected to NP
          Timers : Uptime / Expires
          Interface state : Interface, Next - Hop, State / Mode
(*, 234.1.1.1), 0:0:4/never, RP Null, flags: SJPC
    Incoming interface: Null, RPF nbr Null
                Outgoing interface list: Null
```

1.3. IGMP 配置

1.3.1.IGMP 简介

IGMP 协议运行在主机和三层交换机之间，用于三层交换机维护组播组是否有组成员。目前，广泛使用是 IGMP 的 Version 1 与 Version 2。

主机使用 IGMP 消息通告本地的组播三层交换机它想接收组播流量的主机组地址。如果

主机支持 IGMPv2，它还可以通告组播三层交换机它退出某主机组。组播三层交换机通过 IGMP 协议维护一张主机组成员表，并定期的探询是否有主机组成员存在。

IGMP 消息被置于 IP 报文中传送。IGMPv1 的报文如图 1-3 所示。IGMPv1 中定义了两种消息类型：主机成员询问和主机成员报告。当某主机想要介绍某个组播流量时，它向本地的组播三层交换机发送“主机成员报告”消息，告知欲接收的组播地址。组播三层交换机收到“主机成员报告”消息后把该主机加入指定的主机组，并在设定的周期内向组播地址 224.0.0.1（代表所有支持组播的主机）发送“主机成员询问”消息。主机如果还想继续接收组播流量，必须发送“主机成员报告”消息。

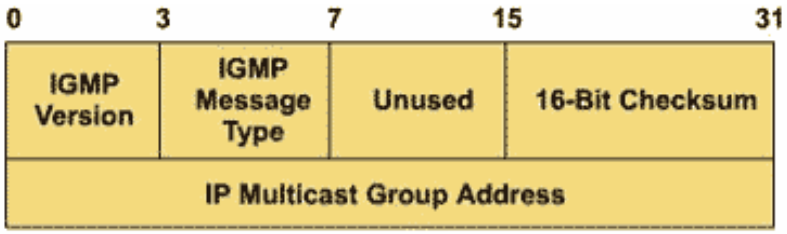


图 1–3 IGMPv1 的报文结构图

IGMPv2 的报文如图 1-4 所示。与 IGMPv1 不同的是它将版本字段和消息类型字段融合，把未使用字段作了“最大响应时间”字段。IGMP Version 2 指定三种报文类型：组成员查询报文、组成员报告报文和组成员离开报文。其中：

- 组成员查询报文：根据组地址不同又分为普通查询报文、特定组查询报文。三层交换机通过普通查询报文来了解网络上有哪些组播成员；特定组查询报文用于对某个特定的组播组的成员进行查询，可以避免属于其它组播组的成员发送响应报文。
- 组成员报告报文：当主机接收到一个普通或特定组的组成员查询报文后，将组成员报告以组播方式传送给支持组播的三层交换机。收到组成员报告后，三层交换机将报告中的组成员加入到三层交换机所在网络的组成员列表中。若在特定的响应时间段内，三层交换机未收到任何组成员报告，即可知晓本地没有组成员，就不再将组播报文传送给它所连接的网络。
- 组成员离开报文：当一台主机离开一个组播组时，IGMP 将给网络内所有支持组播的三层交换机发送一个组成员离开报文。

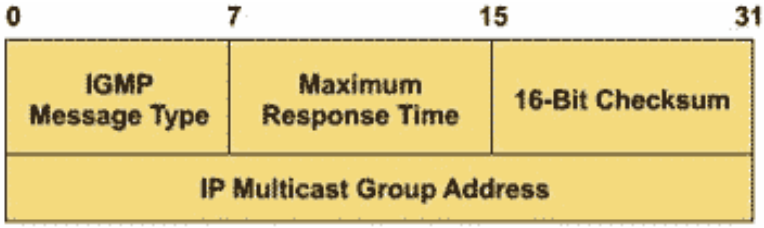


图 1–4 IGMPv2 的报文结构图

IGMPv2 向前兼容 IGMPv1 协议，IGMPv1 的设备可以接收处理 IGMPv2 的消息报文。IGMPv2 中允许三层交换机对指定的主机组地址做“成员询问”，非该组的主机不必响应。如果某主机想退出，它可以主动向三层交换机发送“退出主机组”消息，而不必像 IGMPv1 中那样只能被动退出。

1.3.2.IGMP 配置任务列表

IGMP 的配置任务列表如下：

- 配置三层交换机成为组成员
- 配置 IGMP 的版本号
- 配置 IGMP 主机发送查询报文的时间间隔
- 配置 IGMP 最大查询响应时间
- 配置子网中 Querier 的存活时间

上述的配置任务是可选的，用户可以根据各自的具体需求决定是否进行这些配置。

在接口上加入静态组成员或，或者启动 PIM-DM（**ip pim dense-mode**）或 PIN-SM（**ip pim sparse-mode**），该接口的 IGMP 就自动启动了。IGMP 的关闭只有一种方式，当接口 PIM-DM 或 PIM-SM 关闭且没有静态成员时 IGMP 自动关闭。

1.3.2.1. 配置三层交换机接口成为组成员

通常情况下，运行 IGMP 的主机会对组播三层交换机的 IGMP 查询报文进行响应，如果由于某种原因无法响应，就可能导致组播三层交换机认为该网段没有该组播组地成员，从而取消相应的路径。

为避免这种情况的发生，可以将三层交换机的某个接口配置成为组播组成员，当从该接

口收到 IGMP 查询报文时，由三层交换机进行响应，从而保证接口所在网段能够继续收到组播报文。

配置三层交换机接口成为组成员，不但可使三层交换机模拟主机行为加入组播组，在实际组网中，还可以使静态组播组加入。

表 1–5 配置三层交换机接口成为组成员

命令	命令模式	功能说明
ip igmp join-group *group-address*	接口配置模式	配置三层交换机接口成为组成员。
no ip igmp join-group *group-address*	接口配置模式	将三层交换机接口从组成员中删除。

参数 *group-address* 表示组播组 IP 地址，为 D 类 IP 地址。缺省情况下，三层交换机接口未加入任何组成员。

【示例】配置三层交换机接口成为组 225.2.2.2 的成员。

Tritium(config-vlan-if)# ip igmp join-group 225.2.2.2

1.3.2.2. 配置 IGMP 的版本号

IGMP 各版本之间不能自动转换。因此，同一子网上的所有系统应配置相同的 IGMP 版本，但三层交换机不能自动检测接口当前运行的 IGMP 版本号。

表 1–6 配置 IGMP 版本号

命令	命令模式	功能说明
ip igmp version { **1**|**2**| **3** }	接口配置模式	配置三层交换机接口运行 IGMP 的版本号。
no ip igmp version	接口配置模式	恢复到交换机运行 IGMP 版本号的缺省值。

缺省情况下，三层交换机接口运行 IGMP Version 2。IGMP Version 2 可设置查询报文超时时间和最大查询响应时间。

【示例】配置三层交换机接口运行 IGMP 版本 2。

Tritium(config-vlan-if)# ip igmp version *2*

1.3.2.3. 配置 IGMP 主机发送查询报文的时间间隔

三层交换机需要周期性地向它所连接的网络发送组成员查询报文（Membership Query Message），获得该网段哪些组播组有成员。这个时间间隔由 Query Interval 定时器来设定。

用户可通过配置 Query Interval 定时器修改 IGMP 主机发送查询报文的时间间隔。查询报文发送间隔时间配置必须大于最大查询响应时间时才能生效。在一个网段中有多个组播三层交换机时，由查询器负责向局域网上的所有主机发送 IGMP 查询报文。

表 1–7 配置 IGMP 主机发送查询报文的时间间隔

命令	命令模式	功能说明
ip igmp query-interval *seconds*	接口配置模式	配置 IGMP 主机发送查询报文的时间间隔。
no ip igmp query-interval	接口配置模式	恢复 IGMP 主机发送查询报文时间间隔的缺省值。

参数 *seconds*表示 IGMP host-query 消息的发送时间间隔，取值为 1~18000 之间的整数，单位为秒。缺省情况下 *seconds* 为 60 秒。

【示例】配置 IGMP 主机发送查询报文的时间间隔为 120 秒。

Tritium(config-vlan-if)# ip igmp query-interval *120*

1.3.2.4. 配置 IGMP 最大查询响应时间

当主机收到三层交换机定期发来的查询报文后，会为自己加入的每个组播组都启动一个延时定时器（Delay Timers），采用（0，Max Response Time）之间的一个随机数作为初始值，其中的 Max Response Time 是查询报文指定的最大响应时间（IGMP Version 1 的最大查询响应时间固定为 10 秒）。主机应该定时器超时前，广播组成员报告到三层交换机。若三层交换机在最大查询响应时间超时后还未收到任何组成员报告，就认为已经没有本地组成员，也就不再传送其接收的组播报文到它所连接的网络。合理设置最大响应时间，可以使主机快速响应查询信息，三层交换机也就能快速地掌握组播组成员的存在状况。

请注意：只有当三层交换机接口运行 IGMP Version 2，才能配置该命令。

表 1–8 配置 IGMP 最大查询响应时间

命令	命令模式	功能说明
ip igmp query-max-response-time *seconds*	接口配置模式	配置 IGMP 最大查询响应时间。
no ip igmp query-max-response-time	接口配置模式	恢复 IGMP 最大查询响应时间的缺省值。

参数 *seconds* 表示轮询的最大响应时间，取值为 1~25 之间的整数，单位为秒。最大响应时间的值愈小，三层交换机阻断组的速度愈快。缺省情况下为 10 秒。

【示例】配置 IGMP 最大查询响应时间为 8 秒。

Tritium(config-vlan-if)# ip igmp query-max-response-time *8*

1.3.2.5. 配置查询超时时间

当一个物理网络（可包含多个子网段）上有多台运行 IGMP 的三层交换机时，需要选择一台三层交换机充当查询者 Querier 负责向该物理网络的其它三层交换机发送查询报文。网络初始化时，该物理网络内的所有三层交换机都默认自己为 Querier，并向所连接子网的所有组播主机发送普通查询报文，并将收到查询报文的接口的 IP 地址和发送查询报文接口的 IP 地址比较，物理网络中最小 IP 地址的三层交换机被选为 Querier，其它三层交换机成为非查询者 Non-Querier。

所有非查询者 Non-Querier 启动一个 Other Querier Present Interval 定时器，在定时器超时前，只要收到来自 Querier 的查询报文，定时器就复位。若定时器超时，所有三层交换机都将恢复为 Querier，选举 Querier 的过程重新开始。

需要注意的是：只有当三层交换机接口运行 IGMP Version 2 时，才能进行该项配置。该命令设置 IGMP 查询的超时时间，即在接收到最后一次查询之后，成为查询者需等待的时间。

表 1–9 配置查询超时时间

命令	命令模式	功能说明
ip igmp querier-timeout *seconds*	接口配置模式	配置子网 Querier 的存活时间。
no ip igmp querier-timeout	接口配置模式	恢复子网 Querier 存活时间缺省值。

参数 *seconds* 表示查询超时时间，取值为 10~36000 之间的整数，单位为秒。缺省情况下为 120 秒。

【示例】配置 IGMP 查询超时时间为 30 秒。

Tritium(config-vlan-if)# ip igmp querier-timeout *30*

1.3.3.IGMP 的监控与维护

完成配置后，可执行 **show** 命令显示配置后 IGMP 的运行情况，通过查看显示信息验证配置的效果；执行 **debug** 命令可对 IGMP 进行调试。

表 1–10 IGMP 的监控与维护

命令	命令模式	功能说明
show ip igmp [**vrf** *vrf-name*] **groups** [*group-address*] [*type id*]	特权用户模式	显示与三层交换机直接相连的 IGMP 组播成员信息。
show ip igmp [**vrf** *vrf-name*] **interface** [*type id*]	特权用户模式	显示 IGMP 接口与组播相关的信息。
debug ip igmp [**vrf** *vrf-name*] [*group-address*]	特权用户模式	打开 IGMP 调试信息开关。

【示例】显示与三层交换机相连的 IGMP 组播成员信息。

Tritium# show ip igmp groups

1.4. PIM-DM 配置

1.4.1.PIM-DM 简介

PIM-DM（Protocol Independent Multicast——Dense Mode），协议无关组播——密集模式，主要适用下列几种情况下：

- 发送者和接收者彼此非常接近，并且网络中组播组接收成员的数量很大；
- 组播包的流量很大；
- 组播包的流量是持续的。

PIM-DM 利用单播路由表，从源端 PIM 三层交换机构建一棵到所有接收端节点的组播转发树（Distribution Tree）。在发送组播包时，PIM-DM 认为网络上所有主机都准备接收组播包，组播源一开始将向网络所有下游节点转发组播包，无组播组成员的节点将剪枝报文通知上游三层交换机不用再向下游节点转发数据。

当新的成员在剪枝区域中出现时，PIM-DM 发送嫁接消息，使被剪枝的路径重新变成转发状态。该机制称为泛洪——剪枝过程，PIM-DM 泛洪——剪枝机制将周期性地不断进行。PIM-DM 在泛洪——剪枝过程中采用了逆向路径转发（Reverse Path Forwarding，RPF）技术：当一个组播包到达的时候，三层交换机首先判断到达路径的正确性。若到达端点是由单播路由指示的通往组播源的端口，那么该组播包被认为是从正确路径而来；否则该组播包将作为冗余报文而被丢弃，不进行组播转发。

PIM-DM 主要包括下列几种报文：

- Hello 报文（PIM Hello Message）：PIM Hello 报文由运行 PIM-DM 协议的三层交换机接口定期发送到同网段其它邻居接口，与 PIM-DM 邻居建立邻居关系。另外，由于 IGMPv1 中需要使用 DR（Designed Router）来发送主机查询报文（Host-Query Message），Hello 报文同时负责为运行 IGMPv1 的三层交换机选择 DR（每个 PIM 三层交换机定期广播发送 Hello 报文，IP 地址较大的三层交换机当选为 DR）。
- 嫁接报文（Graft Message）：主机通过 IGMP 报告报文（Membership Report Message）来通知三层交换机它想加入某个组播组，此时端口向上游三层交换机发送 Graft 报文，上游三层交换机收到 Graft 报文后，就将该端口加入到组播组转发列表中。
- 嫁接应答报文（Graft ACK Message）：上游三层交换机在收到 Graft 报文后，需要向发送此嫁接报文的下三层交换机发送应答报文。
- 剪枝报文（Prune Message）：若三层交换机的接口转发列表为空，或接口转发列表变为空时，就向上游三层交换机发送 Prune 报文，通知上游三层交换机将该三层交换机从其接口邻居列表中删除。
- 断言报文（Assert Message）：一个共享网段可能同时有两个上游三层交换机，若它们都向该网段转发组播包的话，该网段的下游三层交换机可能将收到两份相同的组播包。为避免这种情况，PIM-DM 采用 Assert 消息机制：若三层交换机在一个共享局域网的转发端口收到组播包，它要所运行 PIM-DM 的所有三层交换机（组地址为 224.0.0.13）发送 Assert 报文，下游三层交换机将按一系列规则通过比较 Assert 报文的特定域来决定获胜者：报文 preference 小的三层交换机获胜；若报文的 preference 相同，报文 metric 值小的三层交换机获胜；若报文的 metric 值也相同，IP 地址大的三层交换机获胜。获胜者将作为该网段的转发者，失败者发送出接口剪枝报文。由于 PIM-DM 自身不具备路由发现机制，这使得它不依赖于特定的单播路由协议，协议的实现也比较简单。

1.4.2.PIM-DM 配置任务列表

PIM-DM 配置任务列表如下：

- 启动 PIM-DM 协议

1.4.2.1. 启动/禁用 PIM-DM 协议

PIM-DM 协议需要分别在各个接口配置中启动和关闭，同时也启动和关闭了该接口的 IGMP 协议。接口上配置了 PIM-DM 之后，协议会定期发送 PIM 协议 Hello 报文，并且处理 PIM 邻居发送的协议报文。通常情况下，建议在各个接口上都启动 PIM-DM 协议。此配置必须在使能组播路由之后，才能生效。在接口上启动了 PIM-DM 协议后，不能再对此接口启动 PIM-SM 协议，反之亦然。

表 1–11 使能/禁用 PIM-DM 协议

命令	命令模式	功能说明
ip pim dense-mode	接口配置模式	使能 PIM-DM 协议。
no ip pim dense-mode	接口配置模式	禁用 PIM-DM 协议。

缺省情况下，系统禁用 PIM-DM 协议。

1.4.3.PIM-DM 的监控与维护

在完成配置后，可执行 **show** 命令显示配置后 PIM-DM 的运行情况，通过查看显示信息验证配置的效果。执行 **debug** 命令可对 PIM-DM 进行调试。

表 1–12 PIM-DM 的监控与维护

命令	命令模式	功能说明
show ip pim [vrf *vrf-name***] interface** [*type id*]	特权用户模式	显示 PIM 协议接口信息。
show ip pim [vrf *vrf-name***] neighbor**	特权用户模式	显示 PIM 相邻三层交换机信息。
debug ip pim [vrf *vrf-name***]** [*groups-address* | **assert** | **bsr-rp** | **graft** | **hello** | **join-prune** | **register**]	特权用户模式	打开 PIM 调试信息开关。

1.4.4.PIM-DM 典型配置举例

1.4.4.1. 组网需求

在下图中，Multicast Source 作为组播源，Receiver 1 和 Receiver 2 是该组播组的两个接收成员。

通过配置，在 Receiver 1、Receiver 2 与 Multicast Source 间实现组播。

1.4.4.2. 组网图

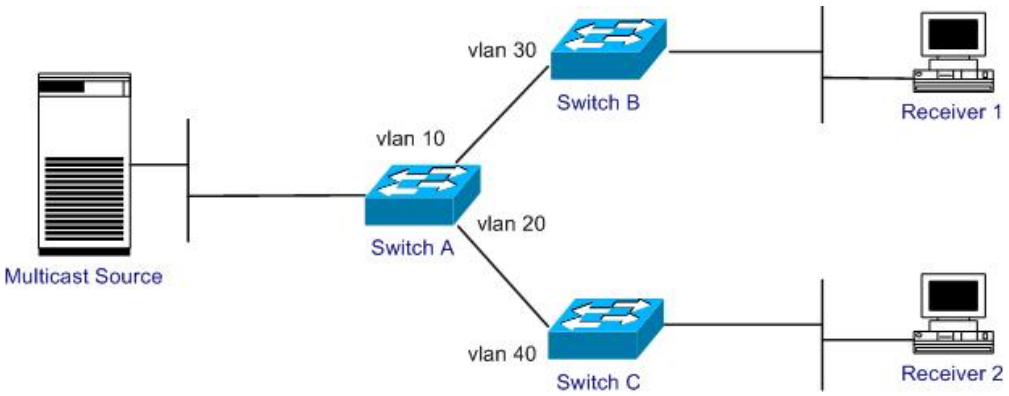


图 1–5 PIM-DM 配置组网图

1.4.4.3. 配置步骤

配置说明：各路由交换机的 VLAN 已经创建好。

（1）配置路由交换机 Switch A

！启动组播。

Tritium(config)# ip multicast-routing

！分别在 VLAN 10 和 VLAN 20 上启动 PIM-DM。

Tritium(config)# interface vlan *10*

Tritium(config-vlan-if)# ip pim dense-mode

Tritium(config-vlan-if)# exit

Tritium(config)# interface vlan *20*

Tritium(config-vlan-if)# ip pim dense-mode

（2）配置路由交换机 Switch B

！启动组播。

Tritium(config)# ip multicast-routing

！在 VLAN 30 上启动 PIM-DM。

Tritium(config)# interface vlan *30*

Tritium(config-vlan-if)# ip pim dense-mode

（3）配置路由交换机 Switch C

！启动组播。

Tritium(config)# ip multicast-routing

！在 VLAN 40 上启动 PIM-DM。

Tritium(config)# interface vlan *40*

Tritium(config-vlan-if)# ip pim dense-mode

1.5. PIM-SM 配置

1.5.1.PIM-SM 简介

PIM-SM（Protocol Independent Multicast，Sparse Mode，协议无关组播——稀疏模式）主要适用于下列几种情况：

- 组成员分布相对分散，范围较广。
- 网络带宽资源有限。

PIM-SM 不依赖于特定的单播路由协议。PIM-SM 假设某个共享网段上的所有三层交换机都不需要发送组播报文，三层交换机只有在主动请求加入某个组播组后，才能收发组播报文。PIM-SM 通过设置 RP（Rendezvous Point——汇聚点）和 BSR（Bootstrap Router——自举三层交换机）向所有支持 PIM-SM 的三层交换机通告组播信息。在 PIM-SM 中，三层交换机显式地加入和退出组播组，可以减少数据报文和控制报文占用的网络带宽。

PIM-SM 构造以 RP 根的共享树 RPT（RP Path Tree），使组播报文能沿着共享树发送。当主机加入一个组播组时，直接连接的三层交换机便向汇聚点（RP）发送 PIM 加入报文；发送者的第一跳三层交换机把发送者注册到 RP 上；接收者的 DR（Designated Router，指定三层交换机）将接收者加入到共享树。使用以 RP 为根的共享树（RPT）进行报文转发，可

以减少三层交换机需要维护的协议状态、提高协议的可伸缩性，降低三层交换机处理开销。当数据流量达到一定程度时，数据可从共享树 RPT（RP Path Tree）切换到基于源的最短路径树 SPT（Short Path Tree），以减少网络延迟。

PIM-SM 主要包括下面几种报文：

- Hello 报文：Hello 报文由运行 PIM-SM 协议的三层交换机接口定期发送到同网段其它邻居接口，与邻居建立邻居关系，还同时为运行 IGMPv1 的版本的三层交换机选择 DR。
- 注册报文：当 DR 收到本地网络上主机发出的组播报文，要将该报文封装在注册报文中单播发送给 RP，以便该报文在 RP 树上分发。注册报文的 IP 头部中的源地址为 DR 的地址，目的地址是 RP 的地址。
- 注册停止报文：由 RP 单播给注册报文的发送者，用来告诉注册报文的发送停止发送注册报文。
- 加入/剪枝报文：该报文被沿着源或 RP 的方向发送上去。加入消息用来建立 RPT 或 SPT，当接收者离开组时用剪枝消息剪枝 RPT 或 SPT。该报文包含各个组播路由项加入和剪枝消息。加入消息和剪枝消息放在一个报文中，但是两种报文中任何一种都可以为空。
- 自举报文：三层交换机要从除了接收到这种报文的接口外的所有的接口发送这种报文。该种报文在 BSR 中产生，并被所有的三层交换机转发。用来向整个 BSR 域通告候选 RP 集。
- 断言报文：在多路访问网络上存在多个三层交换机，并且某个三层交换机路由项的出接口收到组播组报文时，要使用这种报文来指定转发者。
- 候选 RP 信息报文：由候选 RP 定期单播给 BSR，用来通告该候选 RP 服务的组地址集合。

1.5.2.PIM-SM 配置任务列表

PIM-SM 的配置任务列表如下：

- 启动/禁用 PIM-SM 协议

- 配置 BSR 边界
- 指定候选 BSR
- 指定候选 RP
- 配置静态 RP
- 设置从共享树切换到最短路径树的阈值

上述的配置任务中，在使能了组播路由的情况下，启动 PIM-SM 是必须的，其余则是可选的，用户可以根据各自的具体需求决定是否进行这些配置。需要注意的是，在整个 PIM-SM 域中，至少要在一台三层交换机上配置候选 RP 和候选 BSR。

1.5.2.1. 启动/禁用 PIM-SM 协议

PIM-SM 协议需要分别在各个接口上启动和关闭，同时也启动和关闭了该接口的 IGMP 协议。通常情况下，建议各个接口上都应启动 PIM-SM 协议。需要注意的是：PIM-SM 只在指定的接口上运行，一个接口同一时刻只能运行一个组播路由协议。在接口上启动了 PIM-SM 协议后，不能再对此接口启动 PIM-DM 协议，反之亦然。

表 1–13 使能/禁用 PIM-SM 协议

命令	命令模式	功能说明
ip pim sparse-mode	接口配置模式	使能 PIM-SM 协议。
no ip pim sparse-mode	接口配置模式	禁用 PIM-SM 协议。

缺省情况下，系统禁用 PIM-SM 协议。

1.5.2.2. 配置 BSR 边界

设置 BSR 边界后，自举报文（Bootstrap message）不能穿过边界，但其他 PIM 报文可以。通过这种方法，可以分割 PIM-SM 域。缺省情况下，没有设置 BSR 边界。

表 1–14 配置 BSR 边界

命令	命令模式	功能说明
ip pim bsr-border	接口配置模式	配置 BSR 边界。
no ip pim bsr-border	接口配置模式	删除 BSR 边界。

1.5.2.3. 配置接口 DR 优先级

接口 DR 优先级默认为 1。

表 1–15 配置 BSR 边界

命令	命令模式	功能说明
ip pim dr-priority *priority*	接口配置模式	配置接口 DR 优先级，优先级高的当选为 DR。
no ip pim dr-priority	接口配置模式	恢复 DR 默认优先级。

1.5.2.4. 指定候选 BSR

在一个 PIM-SM 域中，必须存在唯一的引导三层交换机 BSR（Bootstrap Router）才能确保 PIM-SM 三层交换机正常工作。BSR 负责收集并发布 RP 信息。多个候选 BSR（Candidate Bootstrap Router，C-BSR）通过自举报文（Bootstrap Message）选举产生唯一公认的 BSR。在得知 BSR 信息之前，C-BSR 认为自己是 BSR，它们定期在 PIM-SM 域中广播（广播地址为 224.0.0.13）自举报文，该报文中包含 BSR 的地址和优先级，使用 BSR 优先级和 IP 地址来选出 BSR，优先级大的为 BSR，如果优先级相同，IP 地址大的为 BSR。候选 BSR 可通过命令来进行配置，C-BSR 应配置在骨干网的三层交换机上。

BSR 是 RP 的管理者，由 BSR 来收集和发布整个网络内的 RP 信息。RP 是通过 BSR 选举产生的。一台三层交换机上只能配置一个接口为 C-BSR。

表 1–16 配置/删除候选 BSR

命令	命令模式	功能说明
ip pim [**vrf** *vrf-name*] **bsr-candidate** *type id* [**mask** *length*] [**priority** *num*]	全局配置模式	配置某接口为候选 BSR。
no ip pim [**vrf** *vrf-name*] **bsr-candidate**	全局配置模式	删除某接口为候选 BSR。

参数说明：

vrf-name：VRF 实例名

type：接口类型，取值为 Loopback、VLAN 之一。

id：Loopback、VLAN ID。

length：掩码长度，取值范围为 0~32。

num：优先级的取值 0~255。

缺省情况下，不指定任何候选 BSR。优先级的缺省值为 0。

1.5.2.5. 配置候选 RP

在 PIM-SM 协议中，路由组播数据创建的共享树 RPT（RP Path Tree）以汇集点 RP（Rendezvous Point）为树根，组成员为叶子。RP 是通过 BSR 选举产生的。在 BSR 选举产生后，所有的 C-RP 定期向 BSR 单播发送 C-RP 广播消息（C-RP Advertisements），由 BSR 选举出 RP 后再向全网扩散发布（可能多个 RP 存在，它们各自有不同的组服务范围），这样所有的三层交换机上都可得到 RP 信息。

在配置候选 RP 时，可以指定 RP 所服务组的范围，它可为所有组播组服务，也可只为其中一部分组播组服务。

表 1–17 配置候选 RP

命令	命令模式	功能说明
ip pim [**vrf** *vrf-name*]**rp-candidate** *type* id] [**group-list** *list-num*] [**priority** *num*] [**interval** *period*]	全局配置模式	配置某接口为候选 RP。
no ip pim [**vrf** *vrf-name*] **rp-candidate**	全局配置模式	删除某接口为候选 RP。

参数说明：

vrf-name：vrf 实例名

type：接口类型，取值为 Loopback、VLAN 之一。

id：Loopback、VLAN ID。

list-num: 标准访问控制列表号<1,99>

num：优先级的取值 0~255。

period：Cand-RP 通告报文的时间间隔，取值 1~65535，单位秒。

缺省情况下，未配置任何接口为候选 RP。

一个网络中可以配置多个 C-RP，RP 优先级越小则优先级越高，同优先级下 HASH 值越大越优先，优先级和 HASH 值相同条件下，IP 地址越大越优先，各组播三层交换机通过动态学习到的 RP 映射选择出最优的 C-RP，作为所有组播组的 RP 地址。

RP 的放置位置对 PIM-SM 模式下组播网络转发及性能有一定影响，通常情况下将 RP 放置在该组播网络中心位置可以使 PIM-SM 模式转发效率更高。

1.5.2.6. 配置静态 RP

该命令为组播路由配置静态 RP 地址，该地址优先于所有学习到的动态 RP 地址，配置后，该三层交换机上所有组播路由采用该地址作为 RP 地址映射建立 RPT。作为静态 RP 的接口必须 UP，使能起 PIM-SM 协议并将该接口网段路由通告出去方能生效。建议在一个 PIM 域中采用动态 RP 选举机制，以适应网络拓扑变化。如果采用静态 RP 配置则需要该 PIM 域所有组播三层交换机都采用静态 RP 地址。

表 1–18 配置静态 RP

命令	命令模式	功能说明
ip pim [**vrf** *vrf-name*] **rp-address** *ip-address list-num*	全局配置模式	为组播路由配置静态 RP。
no ip pim [**vrf** *vrf-name*] **rp-address** *ip-address list-num*	全局配置模式	删除静态 RP 配置。

参数 *ip-address* 表示配置为静态 RP 的 IP 地址。

缺省情况下，未配置任何接口为静态 RP。

1.5.2.7. 配置从共享树切换到源最短路径树的阈值

PIM-SM 三层交换机最初通过共享树转发组播数据包，但是如果组播数据通过的速率超过一定的阈值，组播包所经过的最后一跳三层交换机就会发起从共享树到最短路径树的切换过程。

表 1–19 配置从共享树切换到源最短路径树的阈值

命令	命令模式	功能说明
ip pim [**vrf** *vrf-name*]**spt-threshold** { *traffic-rate* **| infinity** } [**group-list** *list-num*]	全局配置模式	配置从共享树切换到源最短路径树的阈值。
no ip pim [**vrf** *vrf-name*] **spt-threshold** [*traffic-rate* **|infinity**] [**group-list** *list-num*]	全局配置模式	恢复系统默认切换阈值配置。

切换阈值单位为 pak/秒，缺省情况下，从共享树切换到源最短路径树的阈值为 0，也就是说当最后一跳三层交换机收到第一个组播数据包后立即切换到最短路径树。

切换阈值既可以全局设定（对所有组生效），也可以对指定范围的组生效，如果转发速率未达到全局切换配置，则不切换，若达到全局切换值，则检查是否配置有“permit”该组的 ACL

切换值配置，如果有且转发速率没达到该局部配置则不切换，否则进行切换。

在 BCM 交换平台，该切换过程并非立即生效，需要等待一个查询周期，周期为 60 秒，一个周期结束以后才会检查转发的计数值是否超过阈值，如果超过才进行切换。

1.5.3.PIM-SM 的监控与维护

在完成配置后，可执行 **show** 命令显示配置后 PIM-SM 的运行情况，通过查看显示信息验证配置的效果。执行 **debug** 命令可对 PIM-SM 进行调试。

表 1–20 PIM-SM 的监控和维护

命令	命令模式	功能说明
show ip [**vrf** *vrf-name*] **pim bsr**	特权用户模式	显示引导三层交换机（BSR）信息。
show ip pim[**vrf** *vrf-name*] **interface** [*type id*]	特权用户模式	显示 PIM 协议接口信息。
show ip pim [**vrf** *vrf-name*] **neighbor**	特权用户模式	显示 PIM 相邻三层交换机信息。
show ip pim [**vrf** *vrf-name*] **rp** [*group-address*]	特权用户模式	显示选举出的 RP 信息。
debug ip pim [**vrf** *vrf-name*] [*group-address* | **assert** | **bsr-rp** | **graft** | **hello** | **join-prune** | **register**]	特权用户模式	打开 PIM 调试信息开关。
clear ip pim [**vrf** *vrf-name*] **rp-mappping** [*group-address*]	特权用户模式	清除指定/全部侯选 RP 映射信息。
show ip pim [**vrf** *vrf-name*] **rp-candidate** [*group-address*]	特权用户模式	显示指定/全部组能被服务的侯选 RP 信息。
show ip pim [**vrf** *vrf-name*] **rp-hash** *group-address*	特权用户模式	显示指定组 RP 映射信息，包括：选举出的 RP 地址，HASH 掩码，侯选 RP 的优先级，地址，HASH 值，超时时间。
clear ip mroute[**vrf** *vrf-name*] { *group-address* | **all** }	特权用户模式	清除组播路由项。参数为组播地址，表示清除指定组的组播路由项；参数为 all，则表示清除当前学习到的所有组播路由项。

1.5.4.PIM-SM 典型配置举例

1.5.4.1. 组网图

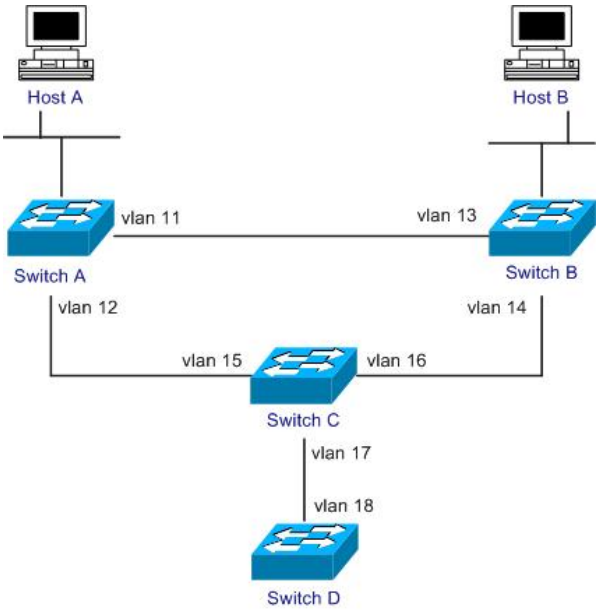


图 1–6 PIM-SM 综合配置图

1.5.4.2. 组网需求

在实际的网络中，由于路由设备由不同的厂商提供，设备上的路由协议也会各不相同。但由于 PIM 协议是独立于特定的单播路由协议的，所以这里我们不关心单播路由协议，假定各个路由交换机之间相互可达。

Host A 是某组播组（组播 IP 地址为：225.0.0.1）的接收者，主机 Host B 现在开始发送目的地址为 225.0.0.1 的数据，路由交换机 A 通过路由交换机 C 接收主机 Host B 发送的组播数据。当 Host B 发送的组播数据的速率超过 100pps 后，将路由交换机 A 加入最短路径树中，直接从路由交换机 B 处接收主机 Host B 发送的组播报文。HOSTA 通过 VLAN10 与 RouterA 相连，HOSTB 通过 VLAN20 与 RouterB 相连。假定 VLAN 成员都是 untag 接口。（如果是 tag 接口，则必须保持 VLAN 在 2 端机器上对应的 VLAN 号必须相同）

1.5.4.3. 配置步骤

（1）配置路由器 Switch A

！启动 PIM-SM。

Tritium(config)# ip multicast-routing

Tritium(config)# interface vlan *11*

Tritium(config-vlan-if)# ip pim sparse-mode

Tritium(config-vlan-if)# exit

Tritium(config)# interface vlan *12*

Tritium(config-vlan-if)# ip pim sparse-mode

Tritium(config-vlan-if)# exit

Tritium(config)# interface vlan *10*

Tritium(config-vlan-if)# ip pim sparse-mode

Tritium(config-vlan-if)# exit

！配置从共享树切换到最短路径树的阈值为 100pps。

Tritium(config)# ip pim spt-threshold *100*

（2）配置路由器 Switch B

！启动 PIM-SM。

Tritium(config)# ip multicast-routing

Tritium(config)# interface vlan *20*

Tritium(config-vlan-if)# ip pim sparse-mode

Tritium(config-vlan-if)# exit

Tritium(config)# interface vlan *13*

Tritium(config-vlan-if)# ip pim sparse-mode

Tritium(config-vlan-if)# exit

Tritium(config)# interface vlan *14*

Tritium(config-vlan-if)# ip pim sparse-mode

（3）配置路由器 Switch C

！启动 PIM-SM。

Tritium(config)# ip multicast-routing

Tritium(config)# interface vlan *15*

Tritium(config-vlan-if)# ip pim sparse-mode

Tritium(config-vlan-if)# exit

Tritium(config)# interface vlan *16*

Tritium(config-vlan-if)# ip pim sparse-mode

Tritium(config-vlan-if)# exit

Tritium(config)# interface vlan *17*

Tritium(config-vlan-if)# ip pim sparse-mode

Tritium(config-vlan-if)# exit

！配置候选 BSR。

Tritium(config)# ip pim bsr-candidate *vlan 13* **mask** *30* **priority** *2*

！配置候选 RP。

Tritium(config)# ip pim rp-candidate *vlan 13*

1.6. PIM sparse-dense 配置

1.6.1.PIM sparse-dense 模式

我们整个组播可以采用 PIM sparse-dense 模式处理机制，运行在 DM 还是 SM 模式是由有无可用的 RP 来决定的，但是 SM 中关键的 BSR 消息只能从 PIM-SM 接口发送出去。

如果没有配置 RP，那么就运行 DM；如果将各接口配置为 SM 模式，并配置了可用的 RP，那么就运行 SM。

为了保持一致，所有一个域内的三层交换机接口模式配置为相同模式。

1.6.2.启动 PIM sparse-dense 协议

PIM sparse-mode 协议需要分别在各个接口配置中启动。

需要注意的是：PIM sparse-dense 只在指定的接口上运行，一个接口同一时刻只能运行一个组播路由协议。

表 1–21 启动 PIM sparse-dense 协议

命令	命令模式	功能说明
ip pim sparse-dense-mode	接口配置模式	启动 PIM sparse-dense 协议。

no ip pim sparse-dense-mode	接口配置模式	启动 PIM sparse-dense 协议。

缺省情况下，系统禁用 PIM sparse-dense 协议。

1.7. MSDP

1.7.1.MSDP 简介

1.7.1.1. MSDP 协议介绍

组播源发现协议（MSDP：Multicast Source Discovery Protocol）描述了一种连接多 PIM-SM（PIM-SM：PIM Sparse Mode）域的机制。每种 PIM-SM 域都使用自己独立的 RP，它并不依赖于其它域内的 RP。该优点在于：

- 不存在第三方（Third-party）资源依赖域内 RP。
- PIM-SM 域只依靠本身的 RP。
- 接收端域：只带接收端的域可以获取数据而不用全局通告组成员。MSDP 可以和其它非 PIM-SM 协议一起使用。

MSDP 描述了多个 PIM-SM 域互连的机制，用于发现其它 PIM-SM 域内的组播源信息。它允许不同域的 RP 共享其组播源信息，并要求域内组播路由协议必须是 PIM-SM。

配置了 MSDP 对等体的 RP 将其域内的活动组播源信息通过 SA（Source Active，活动源）消息通告给它的所有 MSDP 对等体，这样，一个 PIM-SM 域内的组播源信息就会被传递到另一个 PIM-SM 域。

MSDP 对等体可以建立在不同域的 RP 或同一域的多个 RP 之间，也可以建立在 RP 与普通三层交换机之间或者普通路由之间。MSDP 对等体之间使用 TCP 连接。

MSDP 使得一个 PIM-SM 域不需要依赖另一个 PIM-SM 域内的 RP，因为在得到另一个 PIM-SM 域内的组播源信息之后，一个 PIM-SM 域里的接收者可以不通过另一 PIM-SM 域里的 RP 而直接加入到这个域内组播源的 SPT 上。

MSDP 另一个应用是 Anycast RP。在一个域内，用同一个 IP 地址配置不同的三层交换机上的某一接口（通常是 Loopback 接口），同时，配置这些三层交换机上这个接口为候选 RP，并在这些 RP 之间建立 MSDP 对等体关系。单播路由收敛后，组播源可以选择最近的 RP 注册，接收者也可以选择最近的 RP 加入其 RPT。这些 RP 之间通过 MSDP 对等体

了解对方的注册源信息，最终每个 RP 了解到整个域内及域间的所有组播源，这样，每个 RP 上的接收者就可以接收到整个域内及域间的所有组播源发出的组播数据。

通过向就近的 RP 发起注册和 RPT 加入，实现 RP 的负载分担；一个 RP 失效后，其原来注册的源和加入者，又会选择另一个就近的 RP 注册和加入，实现了 RP 的冗余备份。

另外，MSDP 通过 RPF 检查机制，只接受从正确路径上接收到的 SA 消息，避免接受冗余的 SA 消息；可以通过配置 Mesh 全连接组来避免 SA 消息在 MSDP 对等体之间泛滥。

1.7.1.2. 配置注意事项

配置 MSDP 那么必须运行 MBGP，并要求 MSDP 对等体地址与 MBGP 的地址相同，如果不运行 MBGP，则必须配置 MSDP 默认对等体。由于 MSDP 依赖 MBGP 来实行 RPF 检查，因此要求配置的 MSDP 拓扑和 MBGP 要保持一致。

1.7.2.MSDP 配置

1.7.2.1. 配置 MSDP 邻居

配置 MSDP 邻居后，收到的 SA 将向该邻居转发。

表 1–22 配置 MSDP 邻居

命令	命令模式	功能说明
ip msdp [**vrf** *vrf-name*] **peer** *peer-address* [**connect-source** *type id*] [**remote-as**]	全局配置模式	配置 MSDP 邻居。
no ip msdp [**vrf** *vrf-name*] **peer** *peer-address*	全局配置模式	清除 MSDP 邻居。

1.7.2.2. 配置 SA 请求过滤

如果邻居没有缓存 SA，且配置 SA-Request 服务器为自己，会主动向服务器发送 SA 请求通告，该过滤可以过滤掉自己不希望应答的 SA 信息。支持标准访问控制列表，如果不指定访问控制列表，则过滤掉所有 SA-Request 请求。

表 1–23 配置 SA 请求过滤

命令	命令模式	功能说明
ip msdp [**vrf** *vrf-name*] **filter-sa-request** *peer-address* [**list** *list-num*]	全局配置模式	配置 MSDP- 邻居的 sa-request 过滤。

no ip msdp [**vrf** *vrf-name*] **filter-sa-request** *peer-address*	全局配置模式	取消此过滤规则。

1.7.2.3. 配置 SA 过滤策略

缺省情况下，无 SA 过滤。支持标准访问控制列表，如果不指定访问控制列表，则过滤掉所有 in/out SA 信息。

表 1–24 配置 SA 过滤策略

命令	命令模式	功能说明
ip msdp [**vrf** *vrf-name*] **sa-filter** { **in** | **out** } *peer-address* [**list** *list-num*]	全局配置模式	配置 MSDP SA 过滤策略，与其他访问列表处理相同。
no ip msdp [**vrf** *vrf-name*] **sa-filter** { **in** | **out** } *peer-address*	全局配置模式	清除该 SA 过滤设置。

1.7.2.4. 配置 originator-id

只需要在 RP 上配置即可，配置后，SA 中封装的 RP 地址即为该接口地址。

表 1–25 配置 originator-id

命令	命令模式	功能说明
ip msdp [**vrf** *vrf-name*] **originator-id** *type id*	全局配置模式	配置由哪个接口充当 MSDP originator-id。
no ip msdp [**vrf** *vrf-name*] **originator-id**	全局配置模式	取消 originator-id 配置。

1.7.2.5. 配置重连时间

在 MSDP 邻居间 TCP 连接建立前，以该频率重试连接请求。

表 1–26 配置重连时间

命令	命令模式	功能说明
ip msdp [**vrf** *vrf-name*] **timer** *retry-timer*	全局配置模式	设置 MSDP TCP 连接重试时间。
no ip msdp [**vrf** *vrf-name*] **timer**	全局配置模式	恢复默认值 30 秒。

1.7.3.MSDP 维护

1.7.3.1. 清除 MSDP 邻居

清除后，可重新进行 MSDP 连接建立。

表 1–27 清除 MSDP 邻居

命令	命令模式	功能说明
clear ip msdp [**vrf** *vrf-name*] **peer** { *peer-address* | **all**]	特权用户模式	清除指定/全部 MSDP 邻居。

1.7.3.2. 调试 MSDP

如果指定邻居而不指定 debug 类别，则打开/关闭该邻居的所有类型 debug 消息。如果指定类别而不指定邻居，则打开/关闭所有邻居该类别的调试信息。如果同时类别和邻居，则打开/关闭该邻居该类别的调试信息。

表 1–28 调试 MSDP

命令	命令模式	功能说明
debug ip msdp [**vrf** *vrf-name*] *peer-address* **debug ip msdp** [**vrf** *vrf-name*] [*peer-address*] { **fsm** | **keepalive** | **sa** | **sa-request** | **sa-response** }	特权用户模式	打开 MSDP 调试信息。
no debug ip msdp [**vrf** *vrf-name*] *peer-address* **no debug ip msdp** [**vrf** *vrf-name*] [*peer-address*] { **fsm** | **keepalive** | **sa** | **sa-request** | **sa-response** }	特权用户模式	关闭 MSDP 调试信息。

1.7.3.3. 查看 MSDP

在完成配置后，可通过 **show** 命令，查看配置后 MSDP 的运行信息，检查配置的效果。

表 1–29 查看 MSDP

命令	命令模式	功能说明
show ip msdp [**vrf** *vrf-name*] **peer** [*peer-address*]	特权用户模式	显示指定/全部 MSDP 邻居详细信息。
show ip msdp [**vrf** *vrf-name*] **sa-cache**	特权用户模式	显示 MSDP SA 缓存信息。
show ip msdp [**vrf** *vrf-name*] **summary**	特权用户模式	显示 MSDP 邻居概要信息。

1.7.4.MSDP 配置举例

1.7.4.1. 组网说明

SwitchA、SwitchB、SwitchC分别属于3个不同的自治系统，AS号为11、100和101，且分别作为各自AS的RP，组播源与SwitchA连接，组播接收者与SwitchC连接，组播接收者需

要接收由跨AS的组播源发送的数据。

SwtichA loopback1地址1.1.1.1充当AS1 RP；

SwitchB loopback1地址2.2.2.2充当AS2 RP；

SwitchC loopback1地址3.3.3.3充当AS3 RP；

1.7.4.2. 组网图

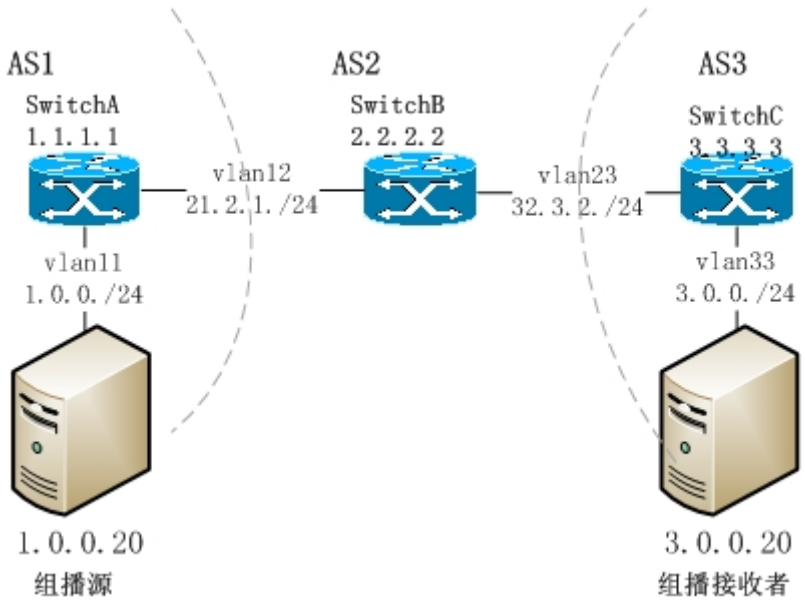


图 1–7 MSDP 示例组网图

1.7.4.3. 配置步骤

首先按以上拓扑配置各接口 IP 地址并使能 ip pim sparse-mode，确认连接正常，PIM 邻居建立正常

将 SwitchA、SwitchB、SwitchC 的 loopback1 分别配置为所在 AS 的 RP，可以采用静态配置，也可以采用动态 BSR-RP 配置

配置 SwitchA 和 SwitchB 的直连接口为 EBGP 邻居，SwitchB 和 SwitchC 的直连接口为 EBGP 邻居，AS1、AS2、AS3 内配置 OSPF 路由并通过 BGP 重发布，保证 SwitchA、SwitchB、SwitchC 能互相学习到其他机器 loopback1 及到组播源的单播路由；

配置 SwitchA 和 SwitchB 的 loopback1 为 MSDP 邻居，SwitchB 和 SwitchC 的 loopback1 为 MSDP 邻居，如 SwitchA 上配置：

Tritium-DUT1(config)#ip msdp peer *2.2.2.2* **connect-source looback** *1*

SwitchB 上配置：

Tritium-DUT1(config)#ip msdp peer *1.1.1.1* connect-source looback *1*

这样 SwitchA 和 SwitchB 就建立了 MSDP 邻居，同样方式配置 SwitchB 和 SwitchC 之间建立 MSDP 邻居；

组播接收者发送 IGMP report，准备接收数据；

组播源发送组播数据，通过 MSDP 邻居传递 SA 信息，建立从 AS1 到 AS3 的转发路径，进行数据转发；

1.8. IGMP-Snooping

1.8.1.IGMP-Snooping 简介

1.8.1.1. IGMP-Snooping 协议介绍

以太网交换机的原理是检测从以太端口来的数据包的源和目的地的 MAC 地址，然后将目的 MAC 地址与交换机系统内部的动态查找表进行比较，以确定发送到哪个端口上，并将数据包发送给相应的目的端口，如果查找不到就从所有端口转发。IGMP snooping 的主要目的是解决局域网交换机组播信息的扩散问题。

1.8.1.2. 配置注意事项

对于网络上不存在接收者，只存在组播源的组播数据，将会向该 VLAN 的所有出端口进行转发.

同一个 VLAN 当中多个端口不能发送同一个组的数据。

1.8.1.3. IGMP SNOOPING 的配置

1.8.1.3.1 配置使能 IGMP SNOOPING 的功能

使能组播路由功能将会自动开启所有 VLAN 的 IGMP SNOOPING 功能

表 1–30 配置使能 IGMP SNOOPING

命令	命令模式	功能说明
ip multicast-routing	全局配置模式	开启组播路由并且使能 IGMP SNOOPING
no ip multicast-routing	全局配置模式	关闭 IGMP SNOOPING

1.8.1.3.2 配置指定端口为路由端口

配置指定的端口为路由端口，数据将向该端口进行转发

表 1–31 配置指定端口为路由器端口

命令	命令模式	功能说明
ip igmp snooping vlan *vlan-id* mrouter interface *name*	全局配置模式	配置 name 指定的端口为 vlan-id 指定 VLAN 的路由端口
no ip igmp snooping vlan *vlan-id* mrouter interface *name*	全局配置模式	取消配置

1.8.1.3.3 配置端口无接收者时立即删除

缺省情况下端口收到接收者发来的离开请求时有最长 2 秒的延迟

表 1–32 配置端口无接收者时立即删除

命令	命令模式	功能说明
ip igmp snooping vlan immediate-leave	全局配置模式	开启立即离开功能
no ip igmp snooping vlan immediate-leave	全局配置模式	取消配置，延迟离开

1.8.1.3.4 配置延迟离开时间长度

延迟时间为 2 倍于 interval,延迟时间内收到接收请求将会取消删除.默认时间为 1 秒。

表 1–33 配置延迟离开时间长度

命令	命令模式	功能说明
Ip igmp snooping vlan vlan-id last-member-query-interval interval	全局配置模式	配置 vlan-id 内的端口延迟时间为 2 * interval
no Ip igmp snooping vlan vlan-id last-member-query-interval interval	全局配置模式	取消配置，使用默认时间

1.8.1.3.5 配置 SNOOPING Querier 功能

配置该功能前需要给 VLAN 配置上 IP 地址，查询消息发送的周期默认为 60 秒，no vlan 以后配置会被清除，下次创建 vlan 的时候需要重新配置。

表 1–34 配置 SNOOPING Querier 功能

命令	命令模式	功能说明
ip igmp snooping querier vlan *vlan-id*	全局配置模式	使能 SNOOPING Querier
no ip igmp snooping querier vlan *vlan-id*	全局配置模式	关闭该功能，也是默认处理
ip igmp snooping vlan *vlan-i***d query-interval** *interval*	全局配置模式	配置查询间隔
no ip igmp snooping vlan *vlan-id* **query-inerval**	全局配置模式	配置查询间隔为默认间隔

1.8.1.4 IGMP SNOOPING 的维护

1.8.1.4.1 清除转发表

清除 Snooping 创建的 2 层转发表

表 1–35 清除转发表

命令	命令模式	功能说明
clear ip igmp snooping vlan *vlan-id*	特权用户模式	清除 VLAN 中所有转发表
clear ip igmp snooping vlan *vlan-id* group *group-address*	特权用户模式	清除 VLAN 中 group- address 对应的转发表.

1.8.1.4.2 调试 IGMP SNOOPING 命令

表 1－36 调试 IGMP SNOOPING 命令

命令	命令模式	功能说明
debug ip igmp snooping	特权用户模式	打开 igmp snooping 调试
no debug ip igmp snooping	特权用户模式	关闭调试

1.8.1.4.3 查看转发表

表 1－37 查看转发表

命令	命令模式	功能说明
show ip igmp snooping vlan *vlan-id*	特权用户模式	显示 VLAN 中所有转发表
show bcm mroute *0.0.0.0 group-address vlan-id*	特权用户模式	查看硬件转发表
show ip igmp snooping mrouter vlan *vlan-id*	特权用户模式	查看路由端口信息

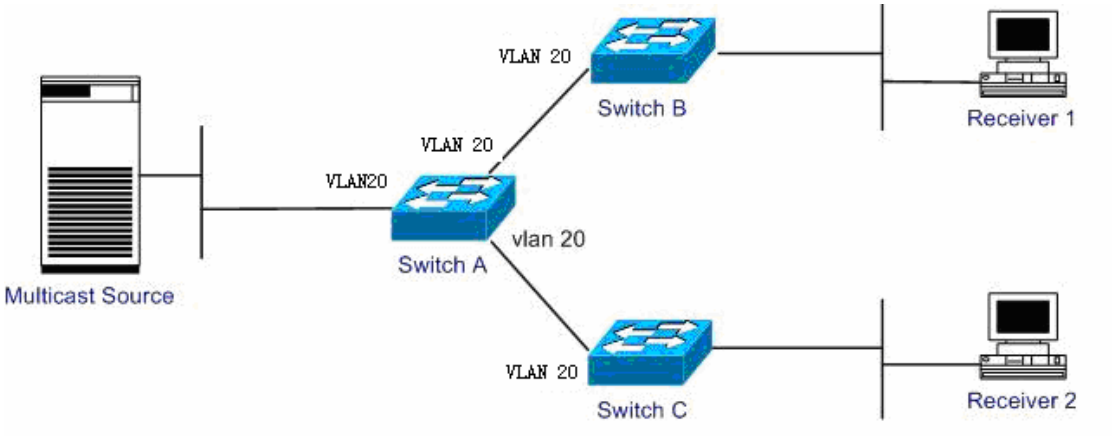
1.8.2.应用举例

1.8.2.1. 组网需求

在下图中，Multicast Source 作为组播源，Receiver 1 和 Receiver 2 是该组播组的两个接收成员。

通过配置，将 Switch A 的三个端口配置到同一个 VLAN 当中，在 Receiver 1、Receiver 2 与 Multicast Source 间通过 IGMP SNOOPING 实现组播数据转发。

1.8.2.2. 组网图



配置步骤

配置说明：各路由交换机的 VLAN 已经创建好，交换机的 B 和 C 连接主机的端口配置为 untaged 端口

（1）配置路由交换机 Switch A

！启动组播时自动启动 SNOOPING

Tritium(config)# ip multicast-routing

（2）开启交换机 VLAN 20 的 Snooping Querier 功能

！必须先给 VLAN20 配置一个 IP 地址

Tritium(config)# interface vlan *20*

Tritium(config-vlan-if)# ip address *192.168.1.1 255.255.0.0*

！开启 VLAN 20 的 Snooping querier 功能

Tritium(config)# ip igmp snooping querier vlan *20*

第2章 IPv6 组播

2.1. MLD

2.1.1.MLD 简介

2.1.1.1. MLD 协议介绍

MLD 是 Multicast Listener Discovery Protocol（组播侦听者发现协议）的简称，它用于 IPv6 设备在其直连网段上发现组播侦听者。组播侦听者（Multicast Listener）是那些希望接收组播数据的主机节点。

设备通过 MLD 协议，可以了解自己的直连网段上是否有 IPv6 组播组的侦听者，并在数据库里做相应记录。同时，设备还维护与这些 IPv6 组播地址相关的定时器信息。MLD 设备使用 IPv6 单播链路本地地址作为源地址发送 MLD 报文。

MLD 使用 ICMPv6（Internet Control Message Protocol for IPv6，针对 IPv6 的互联网控制报文协议）报文类型。所有的 MLD 报文被限制在本地链路上，跳数为 1。

到目前为止，MLD 有两个版本：

MLDv1（由RFC 2710 定义），源自IGMPv2

MLDv2（由RFC 3810 定义），源自IGMPv3

所有版本的MLD 协议都支持ASM（Any-Source Multicast，任意信源组播）模型；MLDv2 可以直接应用于SSM（Source-Specific Multicast，指定信源组播）模型。

目前风云系列设备只支持 MLDv2 版本。

2.1.1.2. MLDv2 简介

1. Ipv6 组播源的过滤

MLDv2 增加了针对IPv6 组播源的过滤模式（INCLUDE/EXCLUDE），使主机在加入某IPv6 组播组G 的同时，能够明确要求接收或拒绝来自某特定IPv6 组播源S的IPv6 组播信息。当主机加入IPv6 组播组时：若要求只接收来自指定IPv6 组播源如S1、S2、……发来的IPv6 组播信息，其报告报文中可以标记为INCLUDE Sources（S1，S2，……）；若

拒绝接收来自指定IPv6 组播源如S1、S2、……发来的IPv6 组播信息，则其报告报文中可以标记为EXCLUDE Sources（S1，S2，……）。

2. Ipv6 接收者信息保存

运行MLDv2 的组播设备按每条直连链路上的组播地址（per multicast address per attached link）来保持IPv6 组播组的状态。IPv6 组播组的状态包括：

过滤模式：保持对INCLUDE 或EXCLUDE 的状态跟踪。

源列表：保持对新增或删除IPv6 组播源的跟踪。

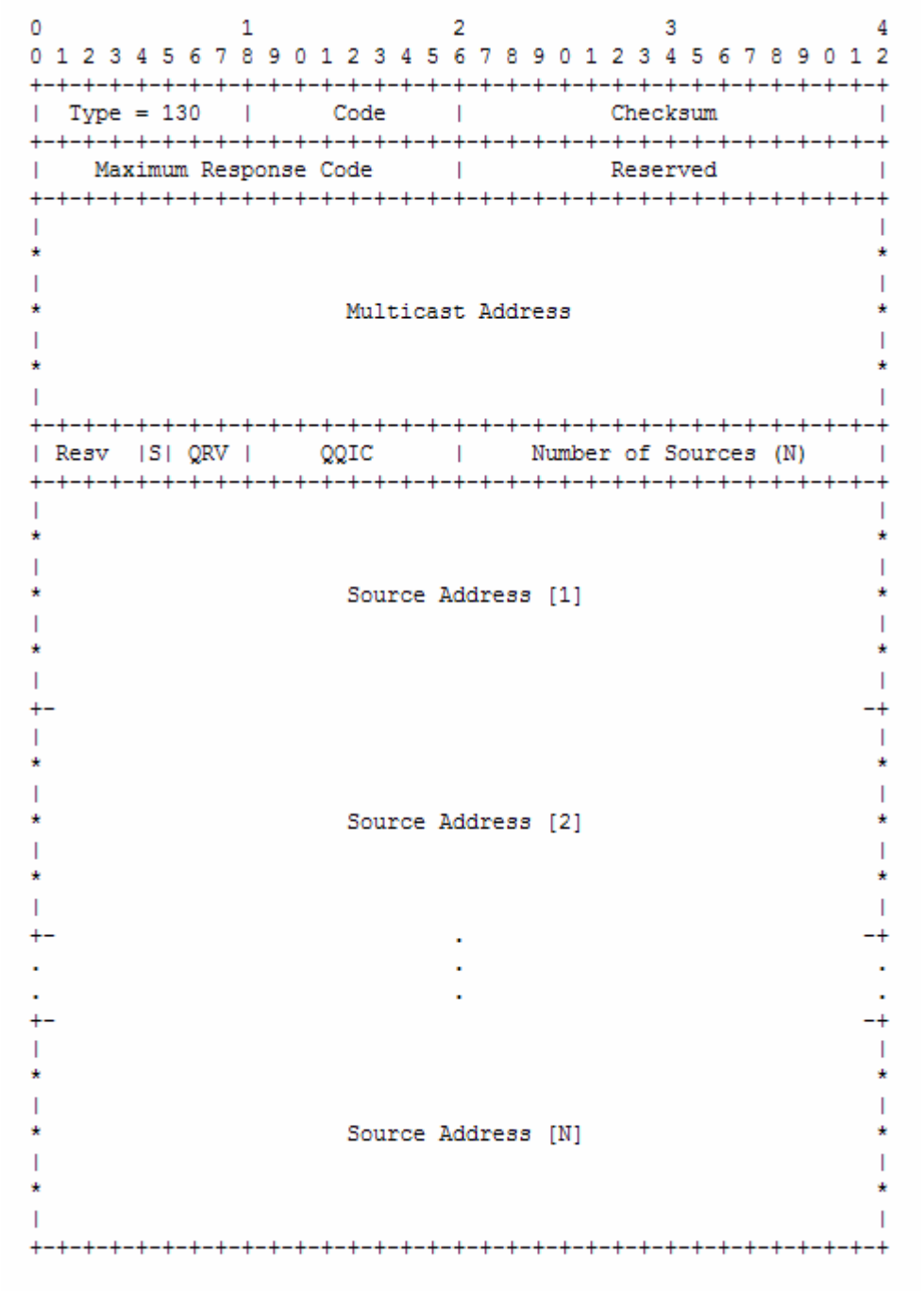
定时器：表示IPv6 组播地址超时后切换到INCLUDE 模式的过滤定时器、关于源记录的源定时器等。

3. 接收者主机的状态监听

运行MLDv2 的组播设备通过侦听接收者主机的状态，记录和维护网段上加入到源组的主机的信息。

2.1.2.MLD 消息格式

2.1.2.1. 查询报文

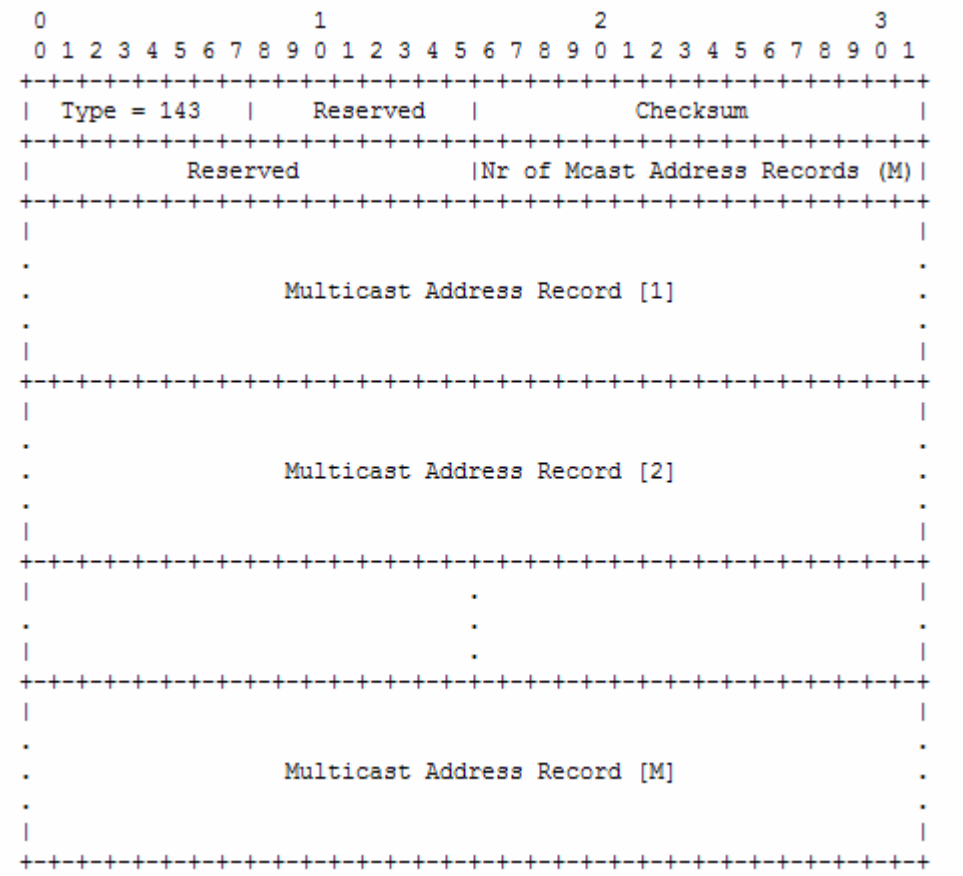


查询报文中各字段的含义

字段	描述
Type=130	报文类型，130 代表查询报文
Code	初始化为0

Checksum	标准的IPv6 校验和
Maximum Response Delay	主机发送报告报文前允许的最大响应时间
Reserved	保留字段，初始化为0
Multicast Address	普遍组查询中，此字段设置为0 特定组或特定源组查询中，设置为待查询的IPv6 组播组地址
S	标识位，表示设备接收到查询报文后是否对定时器更新进行抑制
QRV	查询器的健壮性变量（Querier's Robustness Variable）
QQIC	查询器发送普遍组查询报文的查询间隔（Querier's Query Interval Code）
Number of Sources	普遍组查询或特定组查询中，此字段设置为0 特定源组查询中，此字段表示查询报文中包含的源地址个数
Source Address(i)	特定源组查询中的IPv6 组播源地址（i=1, 2, …, n ， 其中n 表示源地址的个数）

2.1.2.2. 报告报文



MLD 报告报文各字段的值

字段	描述
Type=143	报文类型，143 代表报告报文
Reserved	保留字段，发送时设置为0，接收时忽略此值
Checksum	标准的IPv6 校验和
Number of Multicast Address Records	IPv6 组播地址记录的个数
Multicast Address Record(i)	组播地址记录，表示主机在接口上侦听到的每个IPv6 组播地址信息，包括记录类型、IPv6 组播地址、IPv6 源地址等（i＝1, 2, ..., m，其中m 表示IPv6 组播地址记录的个数）

2.1.3. 配置 MLD 功能

2.1.3.1. 使能/关闭 MLD 功能

使能前的准备

1. 需要使能 MLD 功能的路由接口需要先使能 ipv6
2. 全局配置模式下配置如下命令

命令	命令模式	功能说明
ipv6 multicast-routing	全局配置模式	全局使能 ipv6 组播路由功能

如果上边两个条件任意一个被打破将会关闭 MLD 的功能

2.1.3.2. 配置支持 MLD 的设备发送查询报文的时间间隔

需要周期性地向它所连接的网络发送组成员查询报文（Membership Query Message），获得该网段哪些组播组有成员。这个时间间隔由 Query Interval 定时器来设定。用户可通过配置 Query Interval 定时器修改 MLD 主机发送查询报文的时间间隔。查询报文发送间隔时间配置必须大于最大查询响应时间时才能生效。在一个网段中有多个组播设备时，由查询器负责向局域网上的所有主机发送 MLD 查询报文。

表 2–1 配置支持 MLD 的设备发送查询报文的时间间隔

命令	命令模式	功能说明
Ipv6 mld query-interval *seconds*	接口配置模式	配置 mld 设备发送查询报文的时间间隔。
no Ipv6 mld query-interval	接口配置模式	恢复 mld 设备发送查询报文时间间隔的缺

		省值。

参数 *seconds*表示 MLD 的机器 query 消息的发送时间间隔，取值为 1~3600 之间的整数，单位为秒。缺省情况下 *seconds* 为 125 秒。

【示例】配置 MLD 主机发送查询报文的时间间隔为 120 秒。

Tritium(config-vlan-if)# ipv6 mld query-interval *120*

2.1.3.3. 配置 MLD 最大查询响应时间

当主机收到设备定期发来的查询报文后，会为自己加入的每个组播组都启动一个延时定时器（Delay Timers），采用（0，Max Response Time）之间的一个随机数作为初始值，其中的 Max Response Time 是查询报文指定的最大响应时间（MLD Version 1 的最大查询响应时间固定为 10 秒）。主机应该定时器超时前，广播组成员报告到设备。若设备在最大查询响应时间超时后还未收到任何组成员报告，就认为已经没有本地组成员，也就不再传送其接收的组播报文到它所连接的网络。合理设置最大响应时间，可以使主机快速响应查询信息，设备也就能快速地掌握组播组成员的存在状况。

表 2–2 配置 MLD 最大查询响应时间

命令	命令模式	功能说明
Ipv6 mld query-max-response-time *seconds*	接口配置模式	配置设备最大查询响应时间。
No ipv6 mld query-max-response-time	接口配置模式	恢复设备最大查询响应时间的缺省值。

参数 *seconds* 表示轮询的最大响应时间，取值为 1~32 之间的整数，单位为秒。最大响应时间的值愈小，设备阻断组的速度愈快。缺省情况下为 10 秒。

【示例】配置支持 MLD 的设备最大查询响应时间为 8 秒。

Tritium(config-vlan-if)# ipv6 mld query-max-response-time *8*

2.1.3.4. 配置查询超时时间

当一个物理网络（可包含多个子网段）上有多台运行 MLD 的设备时，需要选择一台设备充当查询者 Querier 负责向该物理网络的其它设备发送查询报文。网络初始化时，该物理网络内的所有设备都默认自己为 Querier，并向所连接子网的所有组播主机发送普通查询报文，并将收到查询报文的接口的 IP 地址和发送查询报文接口的 IP 地址比较，物理网络中最小 IP

地址的设备被选为 Querier，其它设备成为非查询者 Non-Querier。

所有非查询者 Non-Querier 启动一个 Other Querier Present Interval 定时器，在定时器超时前，只要收到来自 Querier 的查询报文，定时器就复位。若定时器超时，所有设备都将恢复为 Querier，选举 Querier 的过程重新开始。

表 2–3 配置查询超时时间

命令	命令模式	功能说明
ipv6 mld querier-timeout *seconds*	接口配置模式	配置子网 Querier 的存活时间。
no ipv6 mld querier-timeout	接口配置模式	恢复子网 Querier 存活时间缺省值。

参数 *seconds* 表示查询超时时间，取值为 60~300 之间的整数，单位为秒。缺省情况下为 255 秒。

【示例】配置 MLD 查询超时时间为 30 秒。

Tritium(config-vlan-if)# ipv6 mld querier-timeout *30*

2.1.3.5. 接口上配置接收者

设备可以在指定的接口上配置需要接收或者不想接收哪些组或者某些源发来的组播数据

表 2–4 接口上配置接收者

命令	命令模式	功能说明
ipv6 mld join-group *ipv6address* [**include** | **exclude** {ipv6_sourceaddr}]	接口配置模式	静态配置 mld 接收者
no ipv6 mld join-group *ipv6address* [**include** | **exclude** {ipv6_sourceaddr}]	接口配置模式	取消静态配置的 mld 接收者

每个组只能配置一种接收模式，配置的时候只能在不配置源，配置 include 方式包含源，配置 exclude 方式包含源三种方式中任选其一,同一个组新的配置方式将会覆盖之前的配置

2.1.3.6. MLD 的监控与维护

表 2–5MLD 的监控与维护

命令	命令模式	功能说明
(no) debug ipv6 mld [*group-address*]	特权模式	打开或者关闭 mld 的调试信息

[*type* {*slot/port* |*id* }]		
show ipv6 mld groups [*group-address* | **detail**]	特权模式	查看 MLD 组信息
show ipv6 mld interface [*type* {*slot/port* |*id* }]	特权模式	显示 mld 接口配置信息

2.1.4. MLD 典型配置举例

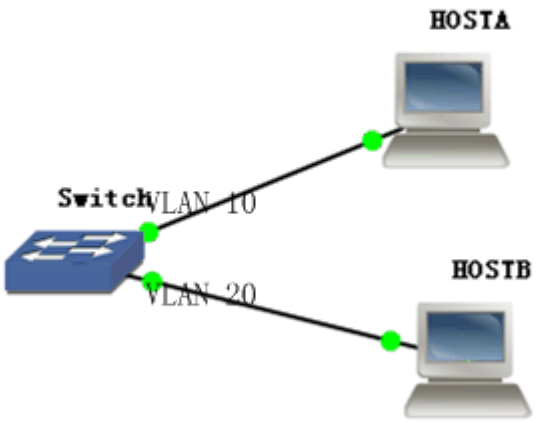
2.1.4.1. 应用描述

以太网络当中有 HOST A, HOST B 这两个接收者：

HOST A 接收(*,FF66::1)的数据

HOST B 接收(2002::1,FF66::2)数据交换机 switch 配置允许接收 MLD 接收请求，会根据 HOST A,HOST B 的请求创建相应的表项

2.1.4.2. 拓扑图



交换机和主机 HOST A 相连的接口配置属于 VLAN10，和 HOST B 的接口配置属于 VLAN 20

2.1.4.3. 配置步骤

1. **交换机的配置：**

Tritium#config

Tritium(config)#ipv6 multicast-routing

Tritium(config)#interface vlan 10

Tritium(config-vlan-if)# ipv6 enable

Tritium(config)#interface vlan 20

Tritium(config-vlan-if)# ipv6 enable

也可以通过配置 ipv6 地址来使能 ipv6

Tritium(config-vlan-if)# ipv6 address 2002::1/16

2. **主机端只需要发送相应的加入请求**

3. **显示接口的 MLD 配置信息**

其中 loopback 0 和 NULL0 是默认使能 Ipv6，所以也使能了 MLD 协议

Tritium# show ipv6 mld interface

Loopback 0 is up

Internet protocol processing enable

MLD is ensabled on interface

MLD query interval is 60 seconds

MLD querier timeout is 255 seconds

MLD max query response time is 10 seconds

Last member query response interval is 1 seconds

MLD querying router is fe80::211:f7ff:fe88:7602(this system)

Null0 is up

Internet protocol processing enable

MLD is ensabled on interface

MLD query interval is 60 seconds

MLD querier timeout is 255 seconds

MLD max query response time is 10 seconds

Last member query response interval is 1 seconds

MLD querying router is fe80::211:f7ff:fe88:7602(this system)

VLAN 10 is up

Internet protocol processing enable

MLD is ensabled on interface

MLD query interval is 60 seconds

MLD querier timeout is 255 seconds

MLD max query response time is 10 seconds

Last member query response interval is 1 seconds

MLD querying router is fe80::211:f7ff:fe66:110d(this system)

VLAN 20 is up

Internet protocol processing enable

MLD is ensabled on interface

MLD query interval is 60 seconds

MLD querier timeout is 255 seconds

MLD max query response time is 10 seconds

Last member query response interval is 1 seconds

MLD querying router is fe80::211:f7ff:fe66:110d(this system)

4.显示接口上的接收者信息

Tritium# show ipv6 mld groups ff66::1 detail

Interface: VLAN 10

Group: ff66::1

Uptime: 0:0:7

Group Mode: EXCLUDE(Expires: 0:6:8)

Last Reporter: fe80::1111:1111

Group source list:

Source list is empty

Tritium# show ipv6 mld groups ff66::2 detail

Interface: VLAN 20

Group: ff66::2

Uptime: 0:0:5

Group Mode: INCLUDE

Last Reporter: fe80::1111:1111

Group source list:

Source Address	Uptime	Expires	Fwd	Flags
2002::1	0:0:5	0:6:10	yes	R

2.2. IPv6 组播路由与转发配置

2.2.1.IPv6 组播转发简介

IPv6 组播实现中，包含组播路由信息表和组播转发表 2 种：

- 组播路由表是通过 IPv6 各种组播协议学习到汇总形成的组播路由信息表，包含详细的组播路由信息；
- 组播转发表是由组播路由信息表生成，用于硬件转发组播数据。

在配置组播路由功能之前，必须首先通过配置单播路由协议，使网内单播路由协议互通，才能正常进行组播转发。

2.2.2.使能 IPv6 组播路由协议

表 2–6 开启/关闭 ipv6 组播路由转发功能

命令	命令模式	功能说明
ipv6 multicast-routing	全局配置模式	全局使能 IPv6 组播路由功能。
no ipv6 multicast-routing	全局配置模式	全局关闭 IPv6 组播路由功能。

该命令全局控制 ipv6 组播路由转发，该命令配置以前，接口上 IPv6 PIM 及 MLD 不能使能，配置该命令后，使能 IPv6 的接口将自动使能 IPv6 PIM 和 IPv6 MLD 功能，同理关闭 IPv6 的接口也将自动关闭 IPv6 PIM 及 MLD 功能。

缺省情况下，系统禁止 IPv6 组播路由转发功能。

2.2.3.IPv6 路由显示和维护

表 2–7IPv6 组播路由显示和维护命令

命令	命令模式	功能说明
show ipv6 mroute [x:x:x:x::x [**source** x:x:x:x::x]]	特权用户模式	显示指定/全部 IPv6 组播路由。
clear ipv6 mroute [x:x:x:x::x]	特权用户模式	清除指定/全部 IPv6 组播路由。
(no)debug ipv6 mroute [x:x:x:x::x]	特权用户模式	打开/关闭 IPv6 组播路由调试信息
(no)debug ipv6 mpacket x:x:x:x::x	特权用户模式	打开/关闭 IPv6 组播报文调试信息

【示例】显示组播路由表信息。

Tritium# show ipv6 mroute

IP Multicast Routing Table

Flags : D - Dense, S - Sparse, s - SSM Group, C - Connected

L - Local, P - Pruned, R - RP - bit set, F - Register flag

T - SPT - bit set, J - Join SPT, N - Injected to NP, M - Mid to CP

Timers : Uptime / Expires

Interface state : Interface, Next - Hop, State / Mode

(*, ff44::), 0:0:6/0:2:54, RP Null, flags: DCL

Incoming interface: Null, RPF nbr Null

Outgoing interface list:

VLAN 10 0:0:6/0:2:54,Forward

2.3. **IPv6 PIM 配置**

2.3.1.IPv6 PIM 简介

IPv6 PIM 是 Protocol Independent Multicast for IPv6 （IPv6 协议无关组播）的简称，表示可以利用静态路由或者任意 IPv6 单播路由协议（包括 RIPng、OSPFv3、IS-ISv6、BGP4+等）所生成的 IPv6 单播路由表为 IPv6 组播提供路由。IPv6 组播路由与所采用的 IPv6 单播路由协议无关，只要能够通过 IPv6 单播路由协议产生相

应的 IPv6 组播路由表项即可。IPv6 PIM 借助 RPF（Reverse Path Forwarding，逆向路径转发）机制实现对 IPv6 组播报文的转发。当 IPv6 组播报文到达本地设备时，首先对其进行 RPF 检查：若 RPF 检查通过，则创建相应的 IPv6 组播路由表项，从而进行 IPv6 组播报文的转发；若 RPF 检查失败，则丢弃该报文。

根据转发机制的不同，IPv6 PIM 分为以下两种模式：

- IPv6 PIM-DM（Protocol Independent Multicast-Dense Mode for IPv6，IPv6 协议无关组播—密集模式）
- IPv6 PIM-SM（Protocol Independent Multicast-Sparse Mode for IPv6，IPv6 协议无关组播—稀疏模式）

稀疏模式下，IPv6 组播区分为以下几种实现：

- IPv6 PIM-SSM：IPv6 源特定组播，由接收者与源直接建立 SPT 转发路径。
- IPv6 PIM-SM：IPv6 任意源组播，由 BSR 公告 RP 信息实现 RPT（共享树）建立。
- IPv6 PIM Embedded-RP：IPv6 任意源组播，由接收者和发送方指定同一地址为 RP，实现 RPT 的建立。

2.3.2.IPv6 PIM 公共配置

2.3.2.1. 使能 IPv6 PIM 协议

IPv6 PIM 协议需要在各个接口使能，接口使能 IPv6 PIM 的前提是：

- 全局使能 IPv6 multicast-routing
- 接口上使能 IPv6

表 2–8 使能/禁用 IPv6 PIM 协议

命令	命令模式	功能说明
ipv6 pim	接口配置模式	使能 IPv6 PIM-SM 协议。
no ipv6 pim	接口配置模式	禁用 IPv6 PIM-SM 协议。
ipv6 pim hello-interval	接口配置模式	配置接口发送 hello 消息的间隔

缺省情况下，系统禁止 IPv6 PIM 协议，当系统使能 IPv6 multicat-routing 后，使能/关闭 IPv6 的接口将自动使能/关闭 IPv6 PIM 协议。

使能 IPv6 PIM 后，系统将根据组范围及有无 RP 映射来确定该接口的每个组播组运行于

哪种 PIM 模式。具体划分如下：

- 使能 IPv6 PIM SSM，则 ff3x::/112 范围运行 PIM-SSM 模式；
- 使能 IPv6 PIM embeded-rp，则 ff7x::/112 范围运行 PIM embedde-rp 模式
- 其他情况下根据有无 RP 映射，决定运行于 IPv6 PIM-SM 还是 IPv6 PIM-DM 模式

2.3.2.2. IPv6 PIM 监控与维护

表 2–9IPv6 PIM 监控和维护

命令	命令模式	功能说明
show ipv6 pim interface	特权用户模式	显示 IPv6 PIM 接口信息。
show ipv6 pim neighbor	特权用户模式	显示 IPv6 PIM 接口邻居信息。

【示例】显示接口 IPv6 PIM 信息。

```
Tritium# show ipv6 pim interface loopback 3
Interface                    PIM   Nbr     Hello   DR
                                   Count   Intvl   Prior

Loopback 3                   on    0       30      1
    Address: fe80::211:f7ff:fe88:7606
    DR: this system
    Addr:
        66::66/112
```

2.3.3.IPv6 PIM-DM 配置

缺省情况下，系统使能 IPv6 multicast-routing 后，使能 IPv6 的接口自动使能 IPv6 PIM-DM 协议。

由于 PIM-DM 协议采用推送（PUSH）模式，直接向所有 PIM 邻居转发组播数据，建立转发路径最快，但因此也会消耗大量带宽，因此建议在符合密集模式转发特点的网络中采用该模式，其他网络中采用稀疏模式转发。

2.3.4.IPv6 PIM-SM 配置

2.3.4.1. IPv6 PIM 配置任务列表

PIM-SM 的配置任务列表如下：

- 启动/禁用 PIM 协议
- 配置 BSR 边界
- 指定候选 BSR
- 指定候选 RP
- 配置静态 RP
- 设置是否进行 SPT 切换

上述的配置任务中，在使能了组播路由的情况下，用户可以根据各自的具体需求决定配置。需要注意的是，在整个 PIM-SM 域中，至少要在一台设备上配置候选 RP 和候选 BSR。

2.3.4.2. 配置 BSR 边界

设置 BSR 边界后，IPv6 PIM 自举（Bootstrap Router）报文不能穿过边界，其他 PIM 协议报文则不受影响，从而完成 IPv6 PIM-SM 域的分割。缺省情况下没有配置 BSR 边界。

表 2–10 配置 IPv6 PIM BSR 边界

命令	命令模式	功能说明
Ipv6 pim bsr-border	接口配置模式	配置 IPv6 PIM BSR 边界。
no ipv6 pim bsr-border	接口配置模式	删除 IPv6 PIM BSR 边界配置。

2.3.4.3. 指定候选 BSR

在一个 IPv6 PIM-SM 域中，必须存在唯一的引导设备 BSR（Bootstrap Router）才能确保 PIM-SM 设备正常工作。BSR 负责收集并发布 RP 信息。多个候选 BSR（Candidate Bootstrap Router，C-BSR）通过自举报文（Bootstrap Message）选举产生唯一公认的 BSR。在得知 BSR 信息之前，C-BSR 认为自己是 BSR，它们定期在 PIM-SM 域中广播（广播地址为 ff02::d）自举报文，该报文中包含 BSR 的地址和优先级，使用 BSR 优先级和 IP 地址来选出 BSR，优先级大的为 BSR，如果优先级相同，IP 地址大的为 BSR。候选 BSR 可通过命令来进行配置，C-BSR 应配置在骨干网的设备上。

BSR 是 RP 的管理者，由 BSR 来收集和发布整个网络内的 RP 信息。IPv6 PIM 的侯选

BSR 必须配置为本地且可用的 IPv6 地址，否则会导致该地址不生效。

表 2–11 配置/删除 IPv6 候选 BSR

命令	命令模式	功能说明
ipv6 pim bsr-candidate x:x:x:x::x [mask-*length*] [**priority** *num*]	全局配置模式	配置某地址为候选 BSR。
no ipv6 pim bsr-candidate	全局配置模式	删除某地址为候选 BSR。

2.3.4.4. 配置侯选 RP

在 PIM-SM 协议中，路由组播数据创建的共享树 RPT（RP Path Tree）以汇集点 RP（Rendezvous Point）为树根，组成员为叶子。RP 是通过 BSR 选举产生的。在 BSR 选举产生后，所有的 C-RP 定期向 BSR 单播发送 C-RP 消息（C-RP Advertisements），由 BSR 选举出 RP 后再向全网扩散发布（可能多个 RP 存在，它们各自有不同的组服务范围），这样所有的设备上都可得到 RP 信息。

在配置候选 RP 时，可以指定 RP 所服务组的范围，它可为所有组播组服务，也可只为其中一部分组播组服务。默认情况下 RP 能服务所有组播组。侯选 RP 地址必须配置为本地且有效的 IPv6 地址，否则将不生效。

表 2–12 配置 IPv6 PIM 候选 RP

命令	命令模式	功能说明
ipv6 pim rp-candidate x:x:x:x::x [group-list *list*][**priority** *num*] [**interval** *period*]	全局配置模式	配置某地址为候选 RP。
no ipv6 pim rp-candidate x:x:x:x::x	全局配置模式	删除某地址为候选 RP。

缺省情况下，未配置任何地址为候选 RP。

一个网络中可以配置多个 C-RP，RP 优先级越小则优先级越高，同优先级下 HASH 值越大越优先，优先级和 HASH 值相同条件下，IP 地址越大越优先，各组播设备通过动态学习到的 RP 映射选择出最优的 C-RP，作为所有组播组的 RP 地址。

RP 的放置位置对 PIM-SM 模式下组播网络转发及性能有一定影响，通常情况下将 RP 放置在该组播网络中心位置可以使 PIM-SM 模式转发效率更高。

默认没有指定 group-list 情况下，该 C-RP 配置可以服务 ff00::/8 所有组播组范围，如果只希望该 C-RP 只为指定组范围服务，则首先配置 IPv6 访问控制列表，将需要服务的范围添加到 permit 项目中（一个 C-RP 最多支持 1000 条 permit 范围配置，多余的则丢弃），然后配置 C-RP 时指定组列表为刚才配置的 IPv6 ACL。

2.3.4.5. 配置静态 RP 地址

该命令为组播路由配置 IPv6 静态 RP 地址，该地址优先于所有学习到的动态 RP 地址，配置后，该设备上所有组播路由采用该地址作为 RP 地址映射建立 RPT。作为静态 RP 的接口必须 UP，使能起 PIM-SM 协议并将该接口网段路由通告出去方能生效。建议在一个 PIM 域中采用动态 RP 选举机制，以适应网络拓扑变化。如果采用静态 RP 配置则需要该 PIM 域所有组播设备都采用相同的静态 RP 地址配置机制。

表 2–13 配置 IPv6 静态 RP

命令	命令模式	功能说明
ipv6 pim rp-address *ipv6-address* [**group-list** *listname*]	全局配置模式	为组播路由配置静态 RP。
no ipv6 pim rp-address *ipv6-address*	全局配置模式	删除静态 RP 配置。

参数 *ipv6-address* 表示配置为静态 RP 的 IP 地址。

缺省情况下，未配置任何接口为静态 RP。

2.3.4.6. 配置从 RPT 向 SPT 切换

IPv6 PIM-SM 设备最初通过共享树转发组播数据包，但是如果组播数据通过的速率超过一定的值，组播包所经过的最后一跳设备就会发起从共享树到最短路径树的切换过程。

表 2–14 配置是否从共享树切换到源最短路径树

命令	命令模式	功能说明
ipv6 pim spt-threshold {*pps* **| infinity} [group-list** *listname***]**	全局配置模式	配置从共享树切换到源最短路径树。
no ipv6 pim spt-threshold	全局配置模式	恢复系统默认切换配置。

缺省情况下，PIM-SM 从共享树切换到源最短路径树，也就是说当最后一跳设备收到第一个组播数据包后立即切换到最短路径树。

当最后一跳进行切换建立 SPT 树失败时，会继续使用 RPT 树转发。

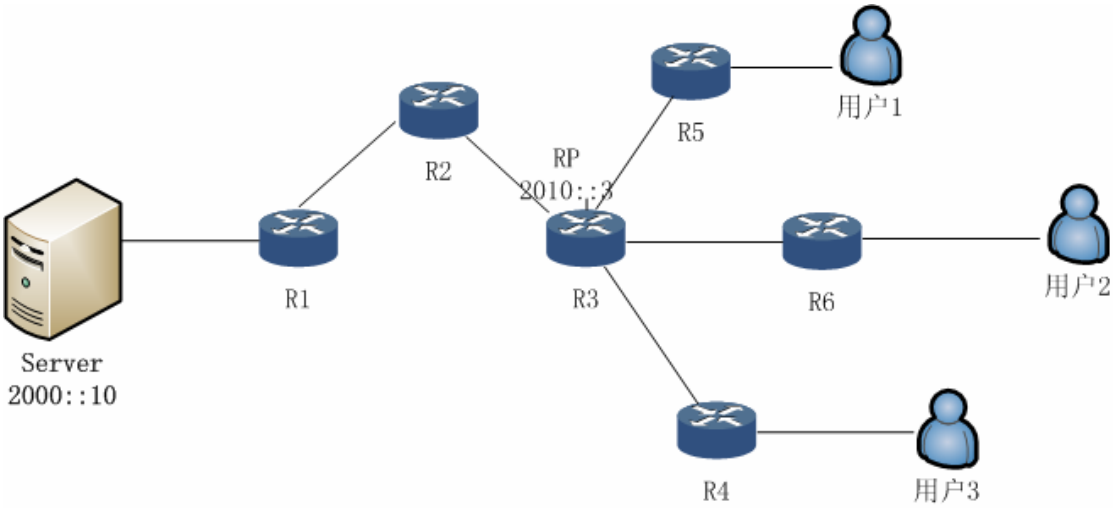
2.3.4.7. PIM-SM 的监控和维护

表 2–15PIM-SM 的监控和维护

命令	命令模式	功能说明
show ipv6 pim bsr	特权用户模式	显示 IPv6 自举设备（BSR）信息及本地侯选 RP 配置信息。
show ipv6 pim rp [*group-address*]	特权用户模式	显示 IPv6 组选举出的 RP 信息。
debug ipv6 pim [*group-address* | **assert** | **bsr-rp** | **graft** | **hello** | **join-prune** | **register**]	特权用户模式	打开 IPv6 PIM 调试信息开关。
show ipv6 pim rp-candidate [*group-address*]	特权用户模式	显示指定/全部组能被服务的侯选 RP 信息。
show ipv6 pim rp-hash *group-address*	特权用户模式	显示指定组 RP 映射信息，包括：选举出的 RP 地址，HASH 掩码，侯选 RP 的优先级，地址，HASH 值，超时时间。

2.3.4.8. PIM-SM 配置举例：

配置拓扑



假定 R5 无法学习到源的单播路由，只能学习到 R3（RP）的单播路由，而 R4 和 R6 能学习到组播源的单播路由。

配置步骤

（1）在所有设备上配置 IPv6 单播路由，使整个网内学习到 RP 的路由，源和 RP 之间的设备能学习到组播源服务器的路由；

（2）各设备及相连的接口上使能 IPv6 multicast-routing，与用户相连的接口使能 IPv6 MLD

（3）在 R3 上配置本地地址 2010::3 并配置如下 BSR、RP 信息：

R3(config)# ipv6 pim bsr-candidate 2010::3

R3(config)# ipv6 pim rp-candidate 2010::3

（4）在该 PIM-SM 域与其他 PIM-SM 域相连的接口配置 IPv6 pim bsr-border

（5）SPT 切换配置：

在无法学习到源路由的 R5 上配置：

R3(config)# ipv6 pim spt-threshold infinity

R5 上不再尝试进行 SPT 切换

R4 和 R6 采用默认切换配置。

（6）show ipv6 pim rp-candidate 观察，确认每台设备都学习到 BSR 和 RP 信息

（7）源发送组播数据，用户发送 MLD report 接收数据

2.3.5.IPv6 PIM-SSM

使能 IPv6 Multicast-routing 后，IPv6 PIM SSM 模式缺省开启，SSM 组范围为 FF3X/12。采用 IPv6 PIM-SSM 转发，需要主机用户端及接口上支持 MLDv2 配置，直接由最后一跳建立到 S 的 SPT 转发路径。

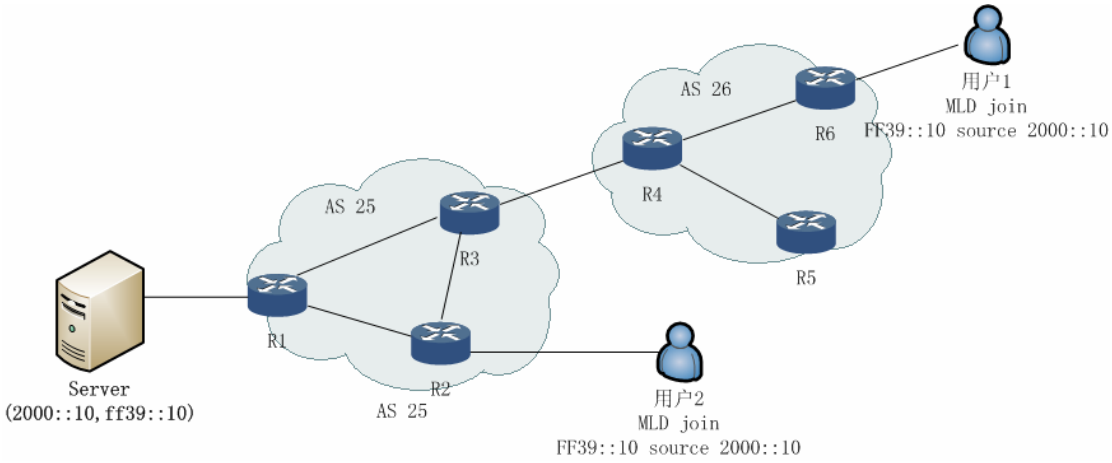
表 2–16IPv6 PIM-SSM 配置命令

命令	命令模式	功能说明
ipv6 pim-ssm	全局配置模式	全局使能 ipv6 PIM-SSM 转发功能。
no ipv6 pim-ssm	全局配置模式	全局关闭 ipv6 PIM-SSM 转发功能。

PIM-SSM 通常用于跨 AS 组播数据转发，在跨 AS 进行转发时，各个 PIM-SM 域的 BSR 不会相互交换 RP 信息，因此，源和接收者并不知道向谁发送注册和加入，PIM-SSM 则不需要 RP 的支持，由连接数据接收者的设备向源发送 SPT join，完成转发路径建立。

2.3.5.1. IPv6 PIM-SSM 配置举例

配置拓扑：



配置步骤：

（1） 在 AS25 和 AS26 图示的所有设备互连接口上使能 IPv6，配置有效的 global 单播地址；并配置适当的单播路由协议，保证自治系统内及系统间单播路由互通；

（2） 各台设备使能 IPv6 multicast-routing，默认即使能 IPv6 PIM-SSM 功能；

（3） 在 R2 和 R6 连接用户的接口上使能 IPv6，IPv6 MLD 将自动使能；

（4） 配置用户支持 MLD 协议，发送 MLDv2 report 加入组 FF39::10, 源列表为

2000::10;

（5） 沿途设备逐跳建立（2000::10, FF39::10）转发项；

组播服务器 2000::10 发送数据，沿 SPT 路径转发给用户 1 和用户 2；

2.4. IPv6 MLD SNOOPING 配置

2.4.1.MLD SNOOPING 简介

MLD Snooping 是 Multicast Listener Discovery Snooping（组播侦听者发现协议窥探协议）的简称。它是运行在二层设备上的 IPv6 组播成员关系监听机制，用于管理和控制 IPv6 组播组，能够让 IPv6 组播数据高效的进行转发.

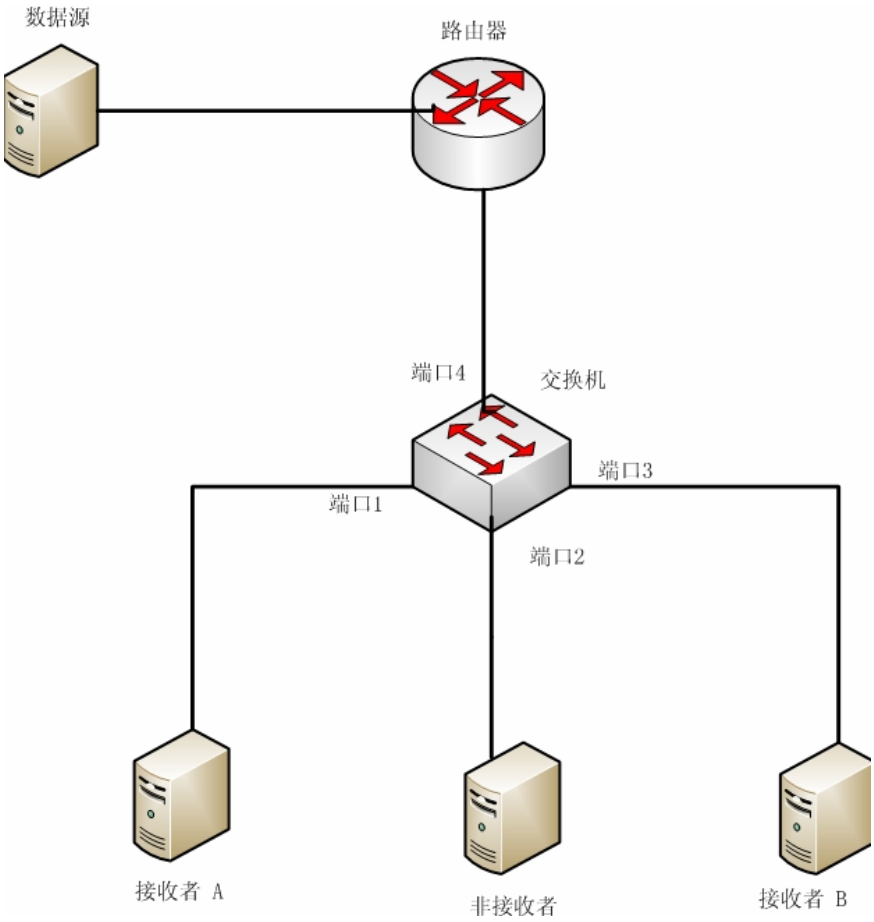
目前支持对 MLDv1，MLDv2 两个版本的 Snooping 功能。

2.4.2.IPv6 MLD-SNOOPING 的配置

运行 MLD Snooping 的二层设备通过对收到的 MLD 报文进行分析，在转发端口和组播目的 MAC 之间建立映射关系，并根据这样的映射关系转发 IPv6 组播数据。

当二层设备没有运行 MLD Snooping 时，IPv6 组播数据报文在二层被广播；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被广播，而是根据网络中实际的组播数据接收者情况，将数据转发到指定的端口上去。

如图所示：



未运行 MLD SNOOPING 状态下，从数据源发送的组播数据到达交换机之后会通过广播的方式向端口 1~3 进行转发。

运行 MLD SNOOPING 协议以后接收者 A,B 通告端口 1，3 接收组播数据，此时端口 2 将不会再收到数据，这样不会造成端口 2 连接的主机丢弃不需要的组播数据报文，减轻了主机的负担.

2.4.3.概念和术语解释

1. MLD 的相关端口

设备端口（Route Port）：

交换机上连接有三层组播路由设备（DR 或MLD 查询器）的端口。交换机将本设备上的所有设备端口都记录在路由端口列表中，可以通过查看命令获知。

主机成员端口（Host Member Port）：

又称IPv6 组播组成员端口，表示交换机上连接IPv6 组播组成员的端口。交换机将本设备上的所有成员端口都记录在MLD Snooping的转发表中，可以通过查看命令获知。

2. 相关的定时器

路由端口超时定时器：

交换机为每个收到 MLD 查询消息的端口设置一个路由端口超时定时器，当定时器超时的时候把端口从设备端口列表中删除，如果静态配置某个端口为路由端口，则该端口不启动定时器，始终保存在路由端口列表当中。

主机端口超时定时器：

当某个端口收到主机的 MLD 加入请求消息时，则该端口为动态主机成员端口，并且启动该定时器，定时器超时之后，将把这个端口从转发列表当中删除掉。收到加入请求会周期性的更新这个定时器。

2.4.4.工作原理

运行了 MLD Snooping 的交换机对不同 MLD 动作的具体处理方式如下：

1. 普遍组查询

设备定期向本地网段内的所有主机与设备（目的地址为 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，交换机将其通过 VLAN 内除接收端口和路由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：

- 如果在设备端口列表中已包含该动态设备端口，则重置其超时定时器。
- 如果在设备端口列表中尚未包含该动态设备端口，则将其添加到设备端口列表中，并启动其超时定时器。

2. 报告成员关系

以下情况，主机会向设备发送 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，它会主动向设备发送 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，交换机将其通过 VLAN 内的所有设备端口转发出去，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，并启动其超时定时器；

- 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，并启动其超时定时器；
- 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，则重置其超时定时器。

说明：

交换机不会将 MLD 成员关系报告报文通过非设备端口转发出去，因为根据 MLD 成员关系报告抑制机制，如果非设备端口下还有该 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，从而使交换机无法获知这些端口下还有该 IPv6 组播组的成员主机。

同时需要注意的是因为 Mld-Snooping 是基于 VLAN ID 和组播 MAC 进行转发，所以通过 MLDv2 的加入消息告知需要接收定的源发来的数据，该组播组的所有源发来的该组播组的数据都会向这个端口进行转发。

3. 离开组播组

当主机离开 IPv6 组播组时，会通过发送 MLD 离开组报文，以通知组播设备自己离开了某个 IPv6 组播组。当交换机从某动态成员端口上收到 MLD 离开组报文时，首先判断离开的 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，交换机只会向路由端口转发该报文，但不做其他处理；
- 如果存在该IPv6 组播组对应的转发表项,且该IPv6 组播组对应转发表项的出端口列表中包含该端口，交换机会将该报文通过 VLAN 内的所有路由端口转发出去。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，所以交换机不会立刻把该端口从该 IPv6 组播组所对应转发表项的出端口列表中删除,而是重置其超时定时器.
- 当设备收到 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。
- 交换机在收到 MLD 特定组查询报文后，将其通过 VLAN 内的所有非路由端口。

对于 MLD 离开组报文的接收端口（假定为动态成员端口），交换机在其超时时间内：

- 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，于是重置其超时定时器；
- 如果没有从该端口收到主机响应该特定组查询的 MLD 成员关系报告报文，则表示该端口下已没有该 IPv6 组播组的成员，则在其超时时间超时后，将其从该 IPv6 组播组所对应转发表项的出端口列表中删除。

2.4.5.配置命令

2.4.5.1. 使能 IPv6 MLD-SNOOPING 协议

IPv6 MLD SNOOPING 协议通过全局配置命令 ipv6 multicast-routing 命令进行配置：

表 2–17 使能/禁用 IPv6 multicast-routing 协议

命令	命令模式	功能说明
ipv6 multicast-routing	全局配置模式	使能 IPv6 Mld Snooping 协议。
no ipv6 multicast-routing	全局配置模式	禁用 IPv6 Mld Snooping 协议。

缺省情况下，系统禁止 IPv6 Mld Snooping 协议.

2.4.5.2. 配置静态路由端口

表 2－18 配置静态路由端口

命令	命令模式	功能说明
Ipv6 mld snooping vlan [*vlan-id***] mrouter [***type id***]**	全局配置模式	开启接口为路由端口
no Ipv6 mld snooping vlan [*vlan-id***] mrouter [***type id***]**	全局配置模式	取消接口为路由端口

2.4.5.3. 配置 MLD SNOOPING 参数

表 2–19 配置 MLD SNOOPING 参数

命令	命令模式	功能说明
ipv6 mld snooping vlan *vlan-id* **immediate-leave**	全局配置模式	使能/关闭 MLD 快速离开功能，收到 leave 后直接删除出接口，不发送查询并等待响应

2.4.5.4. IPv6 MLD SNOOPING 监控与维护

表 2–20IPv6 PIM 监控和维护

命令	命令模式	功能说明
[**no**] **debug ipv6 mld snooping**	特权配置模式	开启/关闭 Mld Snooping 调试。
show ipv6 mld snooping vlan [*vlan-id*] **group**	特权配置模式	显示该 VLAN 的 Mld Snooping 转发表信息。
show ipv6 mld snooping vlan [*vlan-id*] **mrouter**	特权配置模式	显示 Mld Snooping 的路由接口。
clear ipv6 mld snooping vlan *vlan-id* **group [***group-adress*]	特权配置模式	清除该 VLAN 所有/指定 SNOOP 转发表项