H3C MSR 系列路由器

IP 组播配置指导(V7)

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6W103-20140512
产品版本：MSR-CMW710-R0105

前 言

H3C MSR 系列路由器 配置指导(V7)共分为十五本手册，介绍了 MSR 系列路由器各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《IP 组播配置指导》主要介绍组播协议的原理和配置，包括 IGMP、PIM、MSDP、组播 VPN 等 IP 组播相关协议。

前言部分包含如下内容：

适用款型

本手册所描述的内容适用于 MSR 系列路由器中的如下款型：

款型	
MSR 2600	MSR 26-30
MSR 3600	MSR 36-10
	MSR 36-20
	MSR 36-40
	MSR 36-60
	MSR3600-28
	MSR3600-51
MSR 5600	MSR 56-60
	MSR 56-80

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. 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。

3. 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。

4. 端口编号示例约定

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。

产品配套资料

H3C MSR 系列路由器的配套资料包括如下部分：

大类	资料名称	内容介绍
产品知识介绍	路由器产品彩页	帮助您了解产品的主要规格参数及亮点
硬件描述与安装	路由器安装指导	帮助您详细了解设备硬件规格和安装方法，指导您对设备进行安装
	MSR 系列路由器接口模块手册	帮助您详细了解单板的硬件规格
业务配置	MSR 系列路由器配置指导(V7)	帮助您掌握设备软件功能的配置方法及配置步骤
	MSR 系列路由器命令参考(V7)	详细介绍设备的命令，相当于命令字典，方便您查阅各个命令的功能
运行维护	路由器版本说明书	帮助您了解产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

- [服务支持/文档中心]：可以获取硬件安装类、软件升级类、配置类或维护类等产品资料。
- [产品技术]：可以获取产品介绍和技术介绍的文档，包括产品相关介绍、技术介绍、技术白皮书等。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com.cn

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。

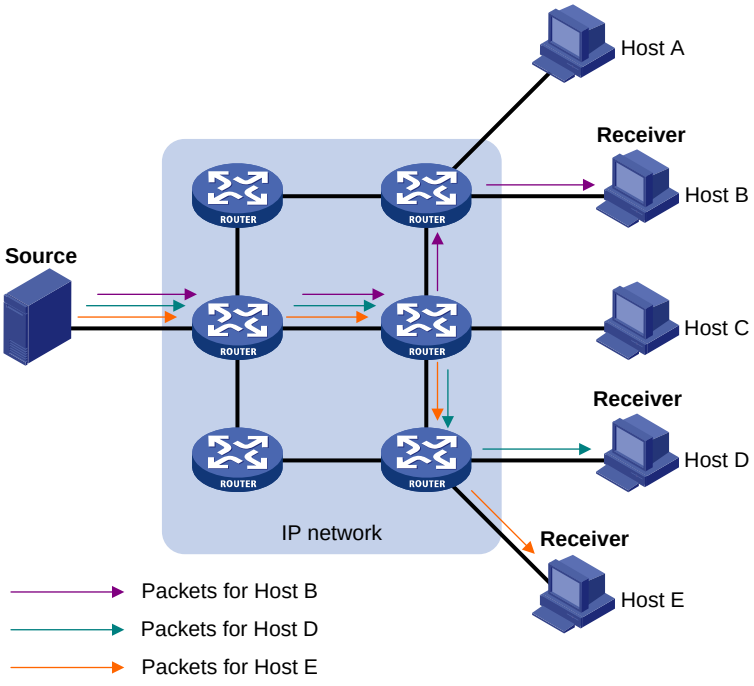
利用组播技术可以方便地提供一些新的增值业务，包括在线直播、网络电视、远程教育、远程医疗、网络电台、实时视频会议等对带宽和数据交互的实时性要求较高的信息服务。

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。

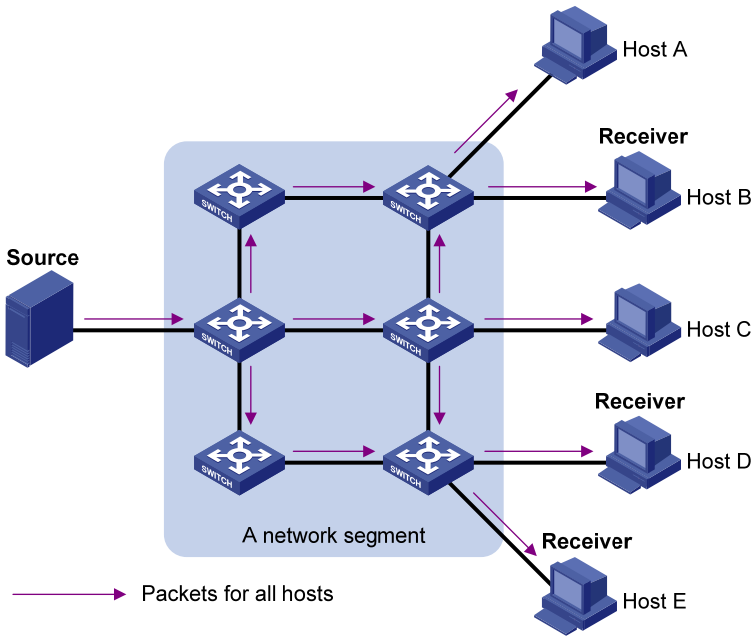
采用单播方式时，网络中传输的信息量与需要该信息的用户量成正比，因此当需要该信息的用户数量较大时，信息源需要将多份内容相同的信息发送给不同的用户，这对信息源以及网络带宽都将造成巨大的压力。

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。

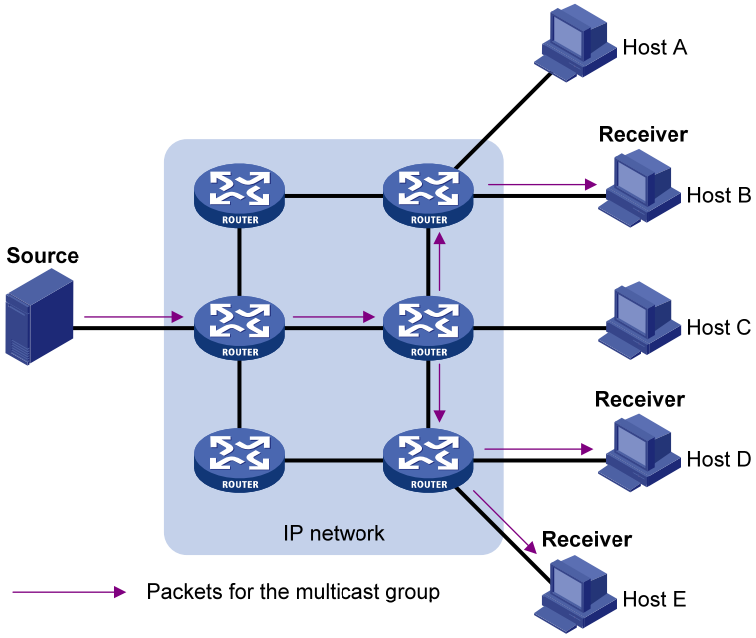
因此，广播方式不利于与特定对象进行数据交互，并且还浪费了大量的带宽。

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。

有关共享树和最短路径树的详细介绍，请参见“IP 组播配置指导”中的“PIM”或“IPv6 PIM”。

1.1.4 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，组播模型分为以下三类：

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。

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。

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：

(1) 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；

(2) 主机注册：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；

(3) 组播路由：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；

(4) 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。

1.3.2 组播地址

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

地址范围	含义
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

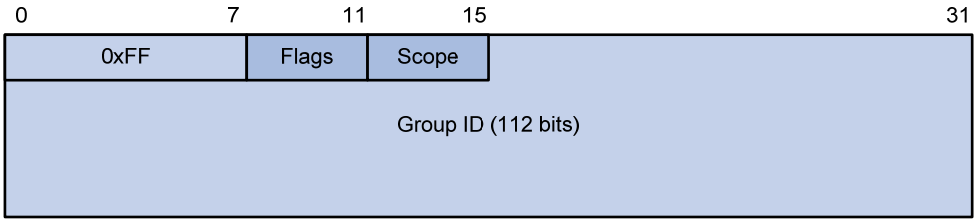
GLOP 是一种 AS（Autonomous System，自治系统）之间的组播地址分配机制，将 AS 号填入该范围内组播地址的中间两个字节中，每个 AS 都可以得到 255 个组播地址。有关 GLOP 的详细介绍请参见 RFC 2770。

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
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
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）

取值	含义
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。

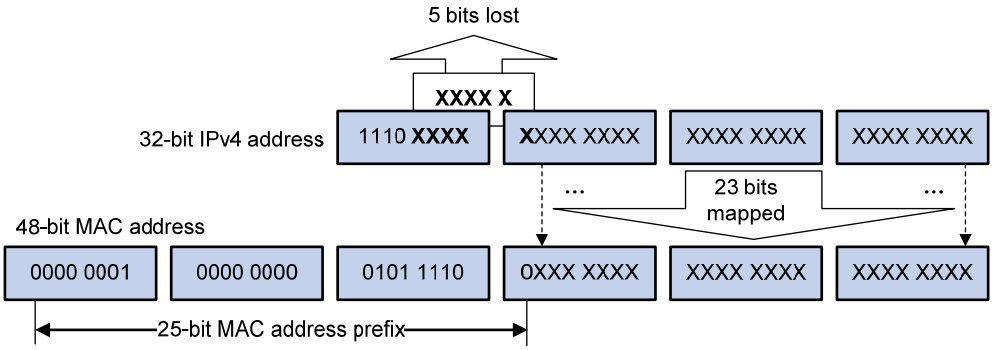
2. 以太网组播MAC地址

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

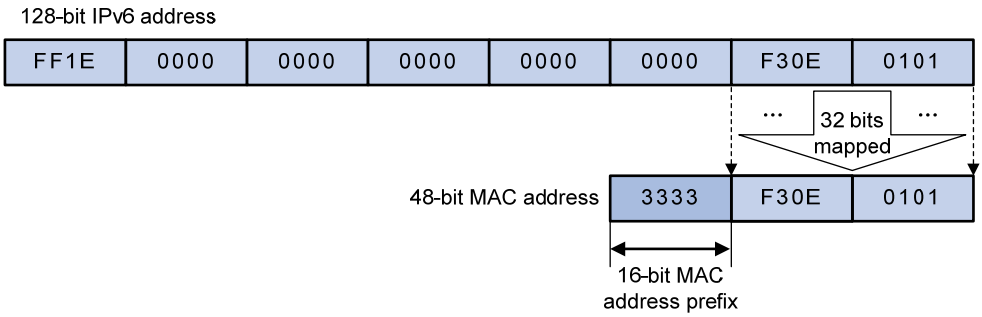


由于 IPv4 组播地址的高 4 位固定为 1110，而低 28 位中只有 23 位被映射到 IPv4 组播 MAC 地址上，从而导致有 5 位信息丢失。于是，将有 32 个 IPv4 组播地址被重复映射到同一个 IPv4 组播 MAC 地址上，因此设备在进行二层处理时，可能会收到一些本不需要的组播数据，这些多余的组播数据就需要上层进行过滤了。

(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



提示

由于 IP 组播地址到组播 MAC 地址重复映射问题的存在，在二层组播转发过程中，设备可能会将组播协议报文当作组播数据报文转发，从而导致组播协议报文无法被正确送达。为了避免这种情况，在组播业务中请勿使用可映射为组播 MAC 地址 0100-5E00-00xx 和 3333-0000-00xx（x 代表任意一个十六进制数）的 IP 组播地址。

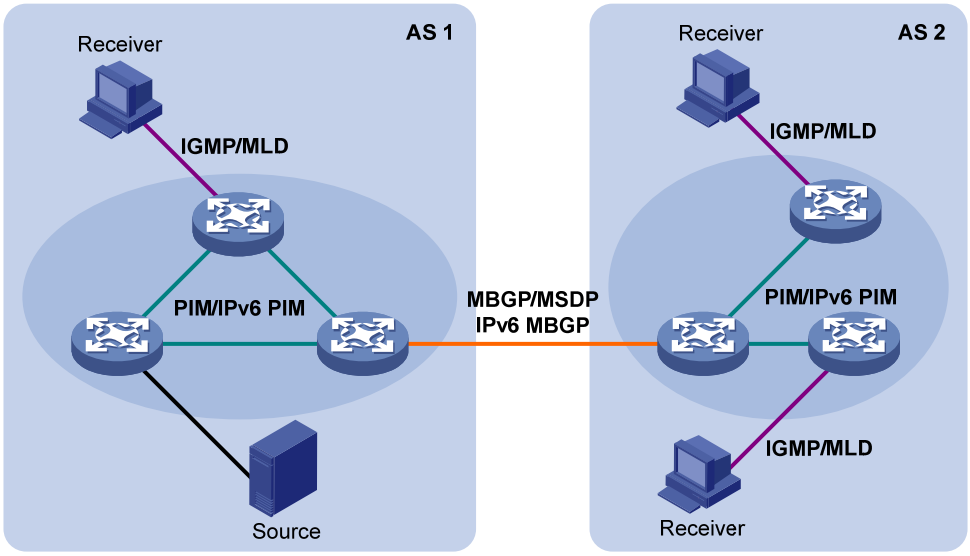
1.3.3 组播协议

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 等。其中，IGMP Snooping、IGMP、PIM、MSDP 和 MBGP 应用于 IPv4；MLD Snooping、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. 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



(1) 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。

(2) 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。

2. 二层组播协议

二层组播协议包括 IGMP Snooping/MLD Snooping 等。

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。

1.4 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”。

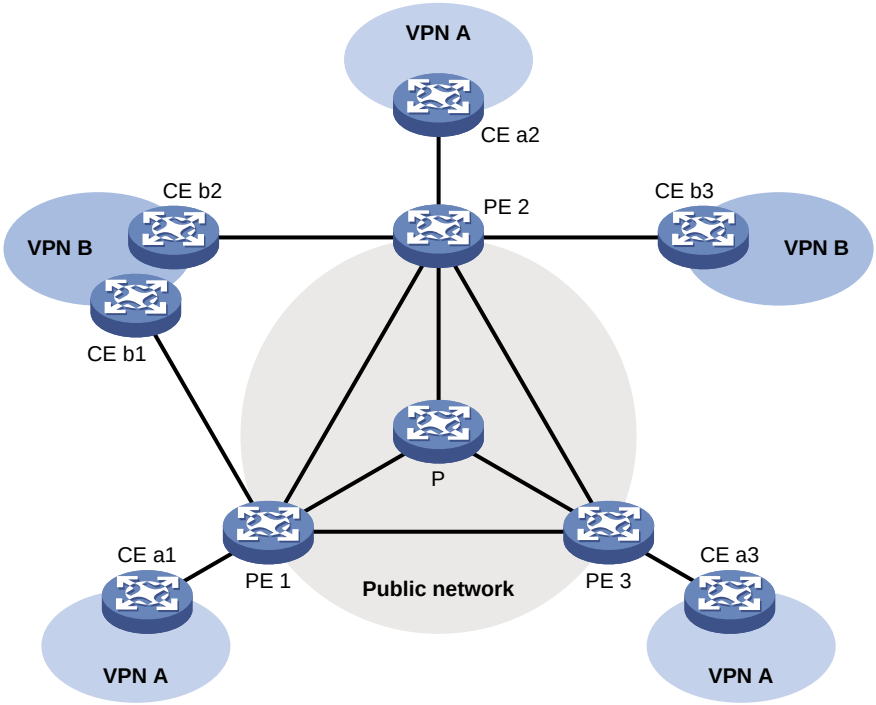
1.5 多实例组播

简单地说，多实例组播就是指在 VPN（Virtual Private Network，虚拟专用网络）中应用的组播。

1.5.1 多实例简介

各VPN网络之间、VPN网络与公共网络之间要求信息隔离。如 图 1-9 所示，VPN A和VPN B通过PE设备接入公共网络。

图1-9 典型的 VPN 组网



- P 设备专属于公网，各 CE 设备则专属于某一 VPN。每台设备只为其专属的网络服务，仅维护一套转发机制。
- PE 设备同时接入公网和 VPN 网络，同时为多个网络服务。在设备上必须严格区分各个网络的信息并为各个网络独立维护一套转发机制。这时，PE 设备上为同一网络服务的一套软硬件设施统称为一个实例（Instance）。PE 设备上同时存在多个实例，而同一个实例也可以分布在多台 PE 设备上。在 PE 设备上，我们将服务于公网的实例称为公网实例，服务于 VPN 的实例则称为 VPN 实例。

1.5.2 多实例在组播中的应用

在 PE 设备上应用多实例组播之后，将具备以下功能：

- 每个实例都独立维护一套组播转发机制：支持各种组播协议，拥有各自独立的 PIM 邻居列表、组播路由表等信息。每个实例转发组播数据时只查找本实例的转发表或路由表；
- 保证各实例之间相互隔离；
- 实现公网实例和 VPN 实例之间的信息交流和数据转换。

以 图 1-9 中的VPN实例A为例，当VPN A中的组播源向某组播组发送组播数据时，在网络中所有可能的接收者中，只有属于VPN A的组播组成员才能收到该组播源发来的组播数据。组播数据在VPN A中以组播方式进行传输，在公网中也以组播方式进行传输。此外，通过配置跨VPN组播转发，还可以使组播数据跨越不同的VPN进行传输。

目 录

1 IGMP Snooping

说明

- 该特性该特性仅在安装了 SIC 4GSW/SIC 4GSWP、DSIC 9FSW/DSIC 9FSWP、HMIM 24GSW/HMIM 24GSW-POE/HMIM 8GSW 二层交换卡的款型和 MSR3600-28/MSR 3600-51 的固定二层接口上支持。
- 文中的交换机指的是安装了二层以太网接口模块的路由器。

1.1 IGMP Snooping简介

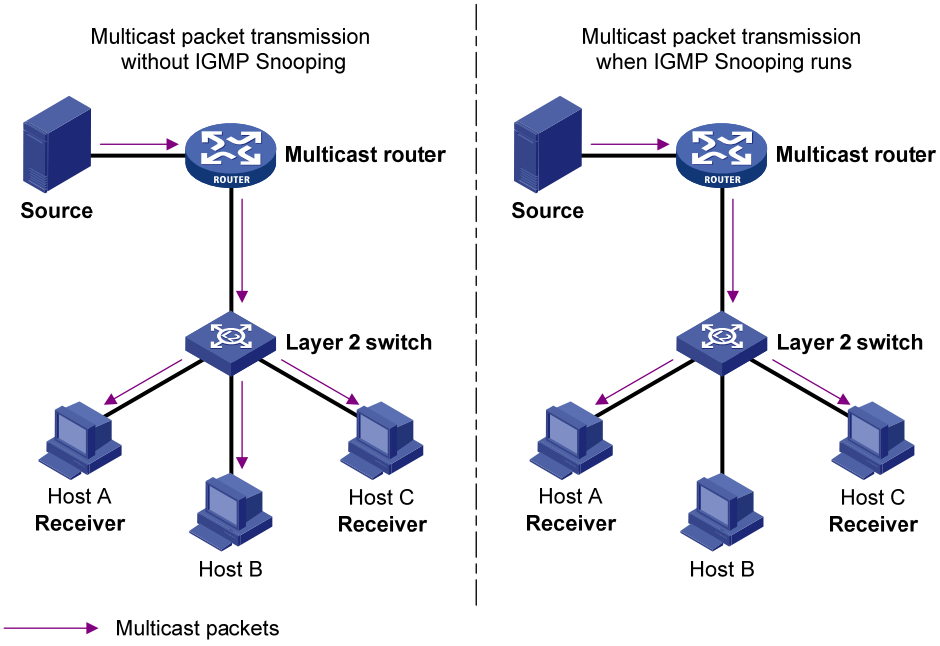
IGMP Snooping（Internet Group Management Protocol Snooping，互联网组管理协议窥探）运行在二层设备上，通过侦听三层设备与主机之间的 IGMP 报文来生成二层组播转发表，从而管理和控制组播数据报文的转发，实现组播数据报文在二层的按需分发。

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：

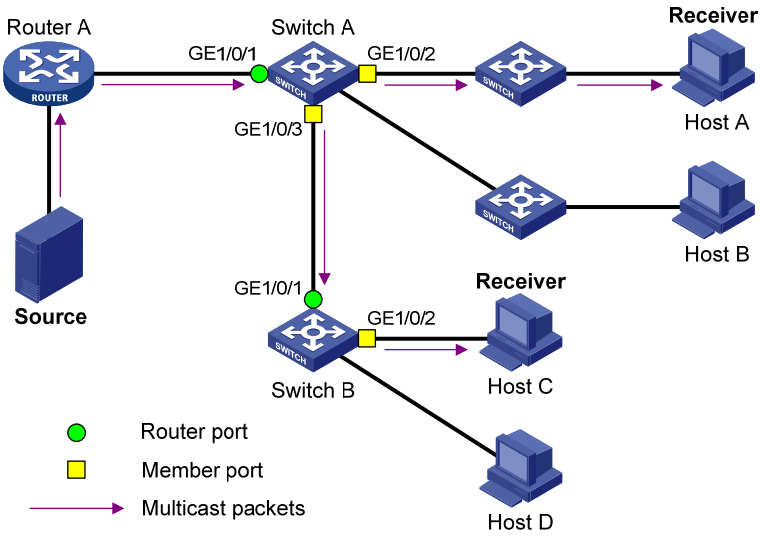
- 减少了二层网络中的广播报文，节约了网络带宽；
- 增强了组播信息的安全性；
- 为实现对每台主机的单独计费带来了方便。

1.1.2 IGMP Snooping基本概念

1. IGMP Snooping相关端口

如 图 1-2 所示，Router A连接组播源，在Switch 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）。

图1-2 IGMP Snooping 相关端口



结合 图 1-2，介绍一下IGMP Snooping相关的端口概念：

- 路由器端口（Router Port）：二层设备上朝向三层组播设备（DR 或 IGMP 查询器）一侧的端口，如 Switch A 和 Switch B 各自的 GigabitEthernet1/0/1 端口。二层设备将本设备上的所有路由器端口都记录在路由器端口列表中。
- 成员端口（Member Port）：又称组播组成员端口，表示二层设备上朝向组播组成员一侧的端口，如 Switch A 的 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 端口，以及 Switch B 的 GigabitEthernet1/0/2 端口。二层设备将本设备上的所有成员端口都记录在 IGMP Snooping 转发表中。

说明

- 本文中提到的路由器端口都是指二层设备上朝向三层组播设备的端口，而不是指路由器上的端口。
- 如不特别指明，本文中提到的路由器/成员端口均包括动态和静态端口。
- 在运行了 IGMP Snooping 的二层设备上，所有收到源地址不为 0.0.0.0 的 IGMP 普遍组查询报文或 PIM Hello 报文的端口都将被视为动态路由器端口。有关 PIM Hello 报文的详细介绍，请参见“IP 组播配置指导”中的“PIM”。

2. IGMP Snooping动态端口老化定时器

表1-1 IGMP Snooping 动态端口老化定时器

定时器	说明	超时前应收到的报文	超时后二层设备的动作
动态路由器端口老化定时器	二层设备为其每个动态路由器端口都启动一个定时器，其超时时间就是动态路由器端口老化时间	源地址不为0.0.0.0的IGMP普遍组查询报文或PIM Hello报文	将该端口从路由器端口列表中删除
动态成员端口老化定时器	当一个端口动态加入某组播组时，二层设备为该端口启动一个定时器，其超时时间就是动态成员端口老化时间	IGMP成员关系报告报文	将该端口从IGMP Snooping转发表中删除

说明

IGMP Snooping 端口老化机制只针对动态端口，静态端口永不老化。

1.1.3 IGMP Snooping工作机制

运行了 IGMP Snooping 的二层设备对不同 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“1.4.3 配置静态端口”。

1. 普遍组查询

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

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

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

2. 报告成员关系

以下情况，主机会向 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。有关主机上的 IGMP 成员关系报告抑制机制的详细介绍，请参见“IP 组播配置指导”中的“IGMP”。

3. 离开组播组

运行 IGMPv1 的主机离开组播组时不会发送 IGMP 离开组报文，因此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对应的转发表项从转发表中删除。

运行 IGMPv2 或 IGMPv3 的主机离开组播组时，会通过发送 IGMP 离开组报文，以通知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包含该端口，二层设备会将该报文通过 VLAN 内的所有路由器端口转发出去。同时，由于并不知道该接收端口下是否还有该组播组的其它成员，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，而是调整该端口的老化定时器。

当 IGMP 查询器收到 IGMP 离开组报文后，从中解析出主机要离开的组播组的地址，并通过接收端口向该组播组发送 IGMP 特定组查询报文。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 协议规范

与 IGMP Snooping 相关的协议规范有：

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

1.2 IGMP Snooping配置任务简介

表1-2 IGMP Snooping 配置任务简介

配置任务		说明	详细配置
配置IGMP Snooping基本功能	使能IGMP Snooping	必选	1.3.2
	配置IGMP Snooping版本	可选	1.3.3
	配置IGMP Snooping转发表项的全局最大数量	可选	1.3.4
配置IGMP Snooping端口功能	配置动态端口老化定时器	可选	1.4.2
	配置静态端口	可选	1.4.3
	配置模拟主机加入	可选	1.4.4
	配置端口快速离开	可选	1.4.5
	禁止端口成为动态路由器端口	可选	1.4.6
配置IGMP Snooping查询器	使能IGMP Snooping查询器	可选	1.5.2
	配置IGMP查询和响应	可选	1.5.3
调整IGMP报文	配置IGMP报文的源IP地址	可选	1.6.2
	配置IGMP报文的802.1p优先级	可选	1.6.3
配置IGMP Snooping策略	配置组播组过滤器	可选	1.7.2
	配置组播数据报文源端口过滤	可选	1.7.3
	配置丢弃未知组播数据报文	可选	1.7.4
	配置IGMP成员关系报告报文抑制	可选	1.7.5
	配置端口加入的组播组最大数量	可选	1.7.6
	配置组播组替换功能	可选	1.7.7

1.3 配置IGMP Snooping基本功能

1.3.1 配置准备

在配置 IGMP Snooping 基本功能之前，需完成以下任务：

- 配置相应 VLAN

在配置 IGMP Snooping 基本功能之前，需准备以下数据：

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

1.3.2 使能IGMP Snooping

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

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

1. 使能指定VLAN内的IGMP Snooping

表1-3 使能指定 VLAN 内的 IGMP Snooping

操作	命令	说明
进入系统视图	**system-view**	-
全局使能IGMP Snooping，并进入IGMP-Snooping视图	**igmp-snooping**	缺省情况下，IGMP Snooping处于关闭状态
使能指定VLAN内的IGMP Snooping	**enable vlan** *vlan-list*	缺省情况下，VLAN内的IGMP Snooping处于关闭状态

2. 在VLAN内使能IGMP Snooping

表1-4 在 VLAN 内使能 IGMP Snooping

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

1.3.3 配置IGMP Snooping版本

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

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

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

1. 配置指定VLAN内的IGMP Snooping版本

表1-5 配置指定 VLAN 内的 IGMP Snooping 版本

操作	命令	说明
进入系统视图	**system-view**	-
进入IGMP-Snooping视图	**igmp-snooping**	-

操作	命令	说明
配置指定VLAN内的IGMP Snooping的版本	**version** *version-number* **vlan** *vlan-list*	缺省情况下，IGMP Snooping的版本为2

2. 在VLAN内配置IGMP Snooping版本

表1-6 在 VLAN 内配置 IGMP Snooping 版本

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

说明

当 IGMP Snooping 的版本由版本 3 切换到版本 2 时，系统将清除所有通过动态加入的 IGMP Snooping 转发表项；对于在版本 3 下通过手工配置而静态加入的 IGMP Snooping 转发表项，则分为以下两种情况进行不同的处理：

- 如果配置的仅仅是静态加入组播组，而没有指定组播源，则这些转发表项将不会被清除；
- 如果配置的是指定了组播源的静态加入组播源组，则这些转发表项将会被清除，并且当再次切换回版本 3 时，这些转发表项将被重新恢复。

有关静态加入的详细配置，请参见“1.4.3 配置静态端口”。

1.3.4 配置IGMP Snooping转发表项的全局最大数量

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

表1-7 配置 IGMP Snooping 转发表项的全局最大数量

操作	命令	说明
进入系统视图	**system-view**	-
进入IGMP-Snooping视图	**igmp-snooping**	-
配置IGMP 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

说明

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

1.4 配置IGMP Snooping端口功能

1.4.1 配置准备

在配置 IGMP Snooping 端口功能之前，需完成以下任务：

- 在 VLAN 内使能 IGMP Snooping

在配置 IGMP Snooping 端口功能之前，需准备以下数据：

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

1.4.2 配置动态端口老化定时器

对于动态路由器端口，如果在其老化时间内没有收到 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。

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

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

说明

如果动态路由器端口收到的是 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。

1. 全局配置动态端口老化定时器

表1-8 全局配置动态端口老化定时器

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

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

2. 在VLAN内配置动态端口老化定时器

表1-9 在 VLAN 内配置动态端口老化定时器

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

1.4.3 配置静态端口

如果某端口所连接的主机需要固定接收发往某组播组或组播源组的组播数据，可以配置该端口静态加入该组播组或组播源组，成为静态成员端口。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。

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

表1-10 配置静态端口

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网	**interface** *interface-type interface-number*	-
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
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

说明

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

1.4.4 配置模拟主机加入

通常情况下，运行 IGMP 的主机会对 IGMP 查询器发出的查询报文进行响应。如果主机由于某种原因无法响应，就可能导致三层组播设备认为该网段没有该组播组的成员，从而取消相应的转发路径。为避免这种情况的发生，可以将二层设备的端口配置成为组播组成员（即配置模拟主机加入）。当收到 IGMP 查询报文时由模拟主机进行响应，从而保证该二层设备能够继续收到组播报文。

模拟主机加入功能的实现原理如下：

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

说明

与静态成员端口不同，配置了模拟主机加入的端口会作为动态成员端口而参与动态成员端口的老化过程。

表1-11 配置模拟主机加入

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网	**interface** *interface-type interface-number*	-
配置模拟主机加入组播组或组播源组	**igmp-snooping host-join** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*	缺省情况下，没有配置模拟主机加入组播组或组播源组

1.4.5 配置端口快速离开

端口快速离开是指当端口收到主机发来的离开指定组播组的 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，当收到针对该组播组的 IGMP 特定组查询报文时，二层设备将不再向该端口转发。

对于一个 VLAN 而言，只有当端口下只有一个接收者时，才可使能端口快速离开功能；否则，若端口下有多个接收者，一个接收者的离开将导致属于同一组播组的其它接收者无法收到组播数据。

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

1. 全局配置端口快速离开

表1-12 全局配置端口快速离开

操作	命令	说明
进入系统视图	**system-view**	-
进入IGMP-Snooping视图	**igmp-snooping**	-

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

2. 在端口上配置端口快速离开

表1-13 在端口上配置端口快速离开

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网	**interface** *interface-type interface-number*	-
在端口上使能端口快速离开功能	**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

1.4.6 禁止端口成为动态路由器端口

目前，在组播用户接入网络中存在以下问题：

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

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

说明

本配置与静态路由器端口的配置互不影响。

表1-14 禁止端口成为动态路由器端口

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网	**interface** *interface-type interface-number*	-
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，不禁止端口成为动态路由器端口

1.5 配置IGMP Snooping查询器

1.5.1 配置准备

在配置 IGMP Snooping 查询器之前，需完成以下任务：

- 在 VLAN 内使能 IGMP Snooping

在配置 IGMP Snooping 查询器之前，需准备以下数据：

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

1.5.2 使能IGMP Snooping查询器

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

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

提示

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

表1-15 使能 IGMP Snooping 查询器

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

1.5.3 配置IGMP查询和响应

可以根据网络的实际情况来修改 IGMP 普遍组查询报文的发送间隔。

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

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

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

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

提示

为避免对组播组成员的误删，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。

1. 全局配置IGMP查询和响应

表1-16 全局配置 IGMP 查询和响应

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

2. 在VLAN内配置IGMP查询和响应

表1-17 在 VLAN 内配置 IGMP 查询和响应

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

1.6 调整IGMP报文

1.6.1 配置准备

在调整 IGMP 报文之前，需完成以下任务：

- 在 VLAN 内使能 IGMP Snooping

在调整 IGMP 报文之前，需准备以下数据：

- IGMP 普遍组查询报文的源 IP 地址
- IGMP 特定组查询报文的源 IP 地址
- IGMP 成员关系报告报文的源 IP 地址
- IGMP 离开组报文的源 IP 地址
- IGMP 报文的 802.1p 优先级

1.6.2 配置IGMP报文的源IP地址

对于收到源 IP 地址为 0.0.0.0 的查询报文的端口，二层设备不会将其设置为动态路由器端口，从而影响数据链路层组播转发表项的建立，最终导致组播数据无法正常转发。当由二层设备充当 IGMP Snooping 查询器时，用户可以通过本配置将 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。

用户也可以通过本配置改变模拟主机或 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。

提示

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。

表1-18 配置 IGMP 报文的源 IP 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
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
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，如果收到过IGMP普遍组查询报文，则以其源IP地址作为IGMP特定组查询报文的源IP地址；否则，采用当前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
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
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

1.6.3 配置IGMP报文的 802.1p优先级

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 报文的 802.1p 优先级。

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

1. 全局配置IGMP报文的 802.1p优先级

表1-19 全局配置 IGMP 报文的 802.1p 优先级

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

2. 在VLAN内配置IGMP报文的 802.1p优先级

表1-20 在 VLAN 内配置 IGMP 报文的 802.1p 优先级

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

1.7 配置IGMP Snooping策略

1.7.1 配置准备

在配置 IGMP Snooping 策略之前，需完成以下任务：

- 在 VLAN 内使能 IGMP Snooping

在配置 IGMP Snooping 策略之前，需准备以下数据：

- 组播组过滤的 ACL 规则
- 端口加入的组播组最大数量

1.7.2 配置组播组过滤器

提示

本配置只对动态组播组有效，对静态组播组无效。

在使能了 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。

在实际应用中，当用户点播某个组播节目时，主机会发起一个 IGMP 成员关系报告报文，该报文到达二层设备后，进行 ACL 检查：如果该接收端口可以加入这个组播组，则将其列入到 IGMP Snooping 转发表中；否则二层设备就丢弃该报文。这样，未通过 ACL 检查的组播数据就不会送到该端口，从而达到控制用户点播组播节目的目的。

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

1. 全局配置组播组过滤器

表1-21 全局配置组播组过滤器

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

2. 在端口上配置组播组过滤器

表1-22 在端口上配置组播组过滤器

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网	**interface** *interface-type interface-number*	-
在端口上配置组播组过滤器	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	缺省情况下，没有配置组播组过滤器，即主机可以加入任意合法的组播组

1.7.3 配置组播数据报文源端口过滤

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：

- 使能该功能后，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。

用户既可在 IGMP-Snooping 视图下对指定端口进行全局配置，也可在接口视图下只对当前端口进行配置，二者的配置优先级相同。

1. 全局配置组播数据报文源端口过滤

表1-23 全局配置组播数据报文源端口过滤

操作	命令	说明
进入系统视图	**system-view**	-
进入IGMP-Snooping视图	**igmp-snooping**	-
使能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，端口上的组播数据报文源端口过滤功能处于关闭状态

2. 在端口上配置组播数据报文源端口过滤

表1-24 在端口上配置组播数据报文源端口过滤

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
使能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，端口上的组播数据报文源端口过滤功能处于关闭状态

说明

该特性仅在安装了 HMIM 24GSW/HMIM 24GSW-POE/HMIM 8GSW 二层交换卡的款型和 MSR3600-28/MSR 3600-51 的固定二层接口上支持。

1.7.4 配置丢弃未知组播数据报文

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

- 当使能了丢弃未知组播数据报文功能时，二层设备将丢弃所有收到的未知组播数据报文；
- 当关闭了丢弃未知组播数据报文功能时，二层设备将在未知组播数据报文所属的 VLAN 内广播该报文。

用户在 VLAN 视图下配置 VLAN 内丢弃未知组播数据报文。

表1-25 在 VLAN 内配置丢弃未知组播数据报文

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

说明

- 对于安装 SIC 4GSW/SIC 4GSWP 二层交换卡的款型，在使能了丢弃未知 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。
- 该特性仅在安装了 SIC 4GSW/SIC 4GSWP、HMIM 24GSW/HMIM 24GSW-POE/HMIM 8GSW 二层交换卡的款型和 MSR3600-28/MSR 3600-51 的固定二层接口上支持。

1.7.5 配置IGMP成员关系报告报文抑制

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

当使能了 IGMP 成员关系报告报文抑制功能后，在一个查询间隔内二层设备只会把收到的某组播组内的第一个 IGMP 成员关系报告报文转发给三层设备，而不继续向三层设备转发来自同一组播组的其它 IGMP 成员关系报告报文，这样可以减少网络中的报文数量。

表1-26 配置 IGMP 成员关系报告报文抑制

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

说明

该特性该特性仅在安装了 HMIM 24GSW/HMIM 24GSW-POE/HMIM 8GSW 二层交换卡的款型和 MSR3600-28/MSR 3600-51 的固定二层接口上支持。

1.7.6 配置端口加入的组播组最大数量

提示

本配置只对动态组播组有效，对静态组播组无效。

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

表1-27 配置端口加入的组播组最大数量

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网	**interface** *interface-type interface-number*	-
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，端口加入的组播组最大数量为4294967295

说明

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

1.7.7 配置组播组替换功能

提示

本配置只对动态组播组有效，对静态组播组无效。

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

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

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

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

1. 全局配置组播组替换功能

表1-28 全局配置组播组替换功能

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

2. 在端口上配置组播组替换功能

表1-29 在端口上配置组播组替换功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网	**interface** *interface-type interface-number*	-
在端口上使能组播组替换功能	**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

1.8 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1-30 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*]
显示动态组播组的IGMP Snooping转发表项信息（MSR 2600/MSR 3600）	**display igmp-snooping group** [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**]
显示动态组播组的IGMP Snooping转发表项信息（MSR 5600）	**display igmp-snooping group** [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
显示动态路由器端口的信息（MSR 2600/MSR 3600）	**display igmp-snooping router-port** [**vlan** *vlan-id*]
显示动态路由器端口的信息（MSR 5600）	**display igmp-snooping router-port** [**vlan** *vlan-id*] [**slot** *slot-number*]
显示静态组播组的IGMP Snooping转发表项信息（MSR 2600/MSR 3600）	**display igmp-snooping static-group** [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**]
显示静态组播组的IGMP Snooping转发表项信息（MSR 5600）	**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（MSR 2600/MSR 3600）	**display igmp-snooping static-router-port** [**vlan** *vlan-id*]
显示静态路由器端口的信息（MSR 5600）	**display igmp-snooping static-router-port** [**vlan** *vlan-id*] [**slot** *slot-number*]
显示IGMP Snooping监听到的IGMP报文统计信息	**display igmp-snooping statistics**
显示二层组播的IP组播组信息（MSR 2600/MSR 3600）	**display l2-multicast ip** [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*]
显示二层组播的IP组播组信息（MSR 5600）	**display l2-multicast ip** [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

操作	命令
显示二层组播的IP转发表信息（MSR 2600/MSR 3600）	**display l2-multicast ip forwarding** [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*]
显示二层组播的IP转发表信息（MSR 5600）	**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（MSR 2600/MSR 3600）	**display l2-multicast mac** [*mac-address*] [**vlan** *vlan-id*]
显示二层组播的MAC组播组信息（MSR 5600）	**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（MSR 2600/MSR 3600）	**display l2-multicast mac forwarding** [*mac-address*] [**vlan** *vlan-id*]
显示二层组播的MAC转发表信息（MSR 5600）	**display l2-multicast mac forwarding** [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]
清除动态组播组的IGMP Snooping转发表项信息	**reset igmp-snooping group** { *group-address* [*source-address*] | **all** } [**vlan** *vlan-id*]
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报文统计信息	**reset igmp-snooping statistics**

1.9 IGMP Snooping典型配置举例

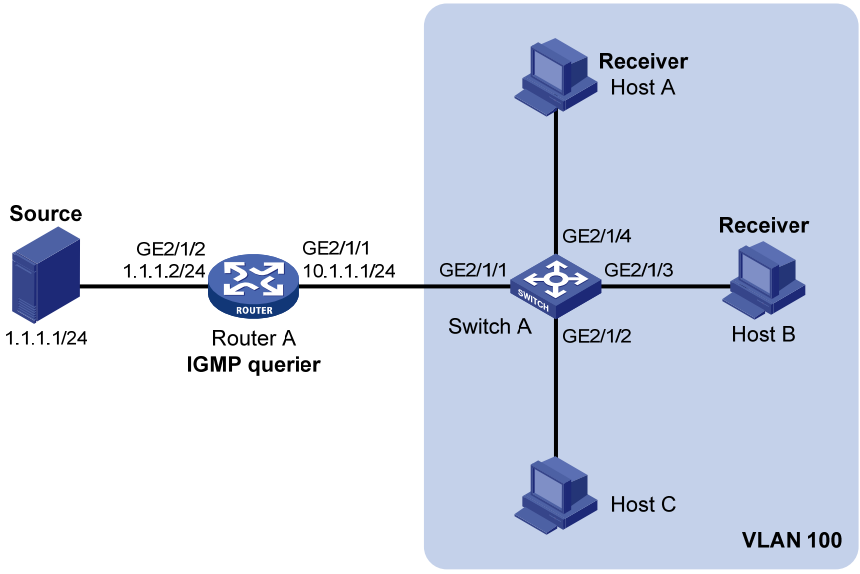
1.9.1 组策略及模拟主机加入配置举例

1. 组网需求

- 如 图 1-3 所示，Router A通过GigabitEthernet2/1/2 接口连接组播源（Source），通过GigabitEthernet2/1/1 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 即使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 GigabitEthernet2/1/3 和 GigabitEthernet2/1/4 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1-3 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 1-3 配置各接口的IP地址和子网掩码，具体配置过程略。

(2) 配置 Router A

使能 IP 组播路由，在接口 GigabitEthernet2/1/2 上使能 PIM-DM，并在接口 GigabitEthernet2/1/1 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] igmp enable
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] pim dm
[RouterA-GigabitEthernet2/1/2] quit
```

(3) 配置 Switch A

全局使能 IGMP Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 到 GigabitEthernet2/1/4 添加到该 VLAN 中；在该 VLAN 内使能 IGMP Snooping，并使能丢弃未知组播数据报文功能。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 2/1/1 to gigabitethernet 2/1/4
[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 number 2001
[SwitchA-acl-basic-2001] rule permit source 224.1.1.1 0
[SwitchA-acl-basic-2001] quit
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] group-policy 2001 vlan 100
[SwitchA-igmp-snooping] quit
```

在 GigabitEthernet2/1/3 和 GigabitEthernet2/1/4 上分别配置模拟主机加入组播组 224.1.1.1。

```
[SwitchA] interface gigabitethernet 2/1/3
[SwitchA-GigabitEthernet2/1/3] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet2/1/3] quit
[SwitchA] interface gigabitethernet 2/1/4
[SwitchA-GigabitEthernet2/1/4] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet2/1/4] 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 内动态组播组的 IGMP Snooping 转发表项信息。

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

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host slots (0 in total):
    Host ports (2 in total):
      GE2/1/3         (00:03:23)
      GE2/1/4         (00:04:10)
```

由此可见，Host A 和 Host B 所在的端口 GigabitEthernet2/1/4 和 GigabitEthernet2/1/3 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。

1.9.2 静态端口配置举例

1. 组网需求

- 如 图 1-4 所示，Router A通过GigabitEthernet2/1/2 接口连接组播源（Source），通过GigabitEthernet2/1/1 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 GigabitEthernet2/1/3 和 GigabitEthernet2/1/5 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 GigabitEthernet2/1/3 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。

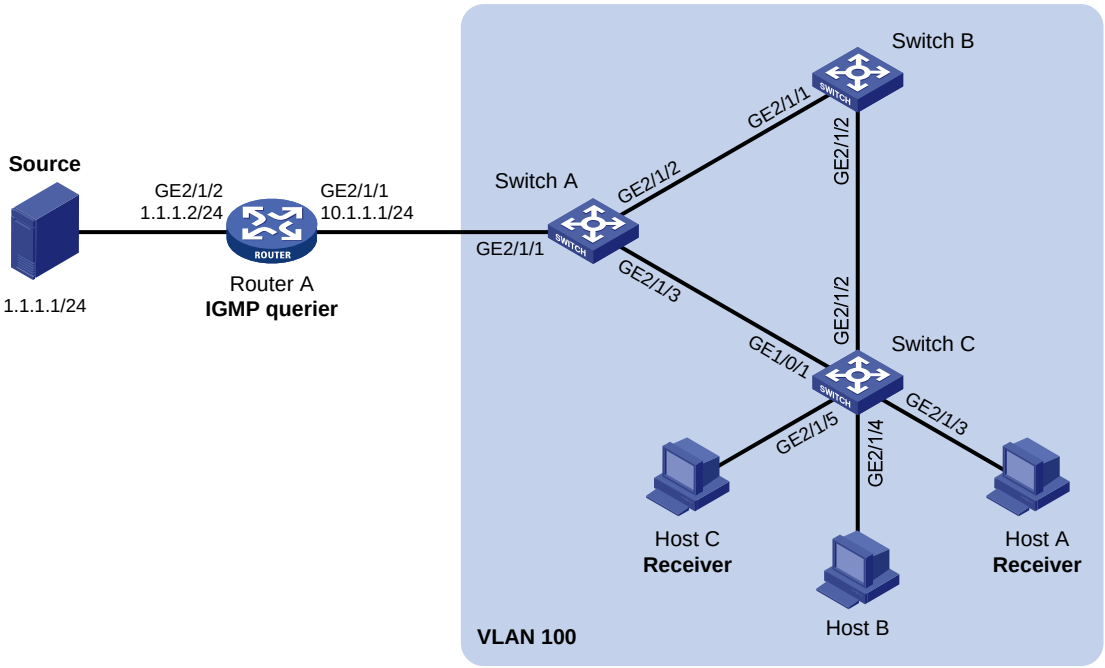
说明

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1-4 静态端口配置组网图



3. 配置步骤

(1) 配置 IP 地址

请按照 图 1-4 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 GigabitEthernet2/1/2 上使能 PIM-DM，并在接口 GigabitEthernet2/1/1 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] igmp enable
[RouterA-GigabitEthernet2/1/1] quit
```

```
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] pim dm
[RouterA-GigabitEthernet2/1/2] quit
```

(3) 配置 Switch A

全局使能 IGMP Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 到 GigabitEthernet2/1/3 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 2/1/1 to gigabitethernet 2/1/3
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] quit
```

把 GigabitEthernet2/1/3 配置为静态路由器端口。

```
[SwitchA] interface gigabitethernet 2/1/3
[SwitchA-GigabitEthernet2/1/3] igmp-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet2/1/3] quit
```

(4) 配置 Switch B

全局使能 IGMP Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping。

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

(5) 配置 Switch C

全局使能 IGMP Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 到 GigabitEthernet2/1/5 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 2/1/1 to gigabitethernet 2/1/5
[SwitchC-vlan100] igmp-snooping enable
[SwitchC-vlan100] quit
```

分别在端口 GigabitEthernet2/1/3 和 GigabitEthernet2/1/5 上配置静态加入组播组 224.1.1.1。

```
[SwitchC] interface gigabitethernet 2/1/3
[SwitchC-GigabitEthernet2/1/3] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-GigabitEthernet2/1/3] quit
[SwitchC] interface gigabitethernet 2/1/5
```

```
[SwitchC-GigabitEthernet2/1/5] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-GigabitEthernet2/1/5] 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 slots (0 in total):
  Router ports (1 in total):
    GE2/1/3
```

由此可见，Switch A 上的端口 GigabitEthernet2/1/3 已经成为了静态路由器端口。

显示 Switch C 上 VLAN 100 内静态组播组的 IGMP Snooping 转发表项信息。

```
[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 slots (0 in total):
    Host ports (2 in total):
      GE2/1/3
      GE2/1/5
```

由此可见，Switch C 上的端口 GigabitEthernet2/1/3 和 GigabitEthernet2/1/5 已经成为了组播组 224.1.1.1 的静态成员端口。

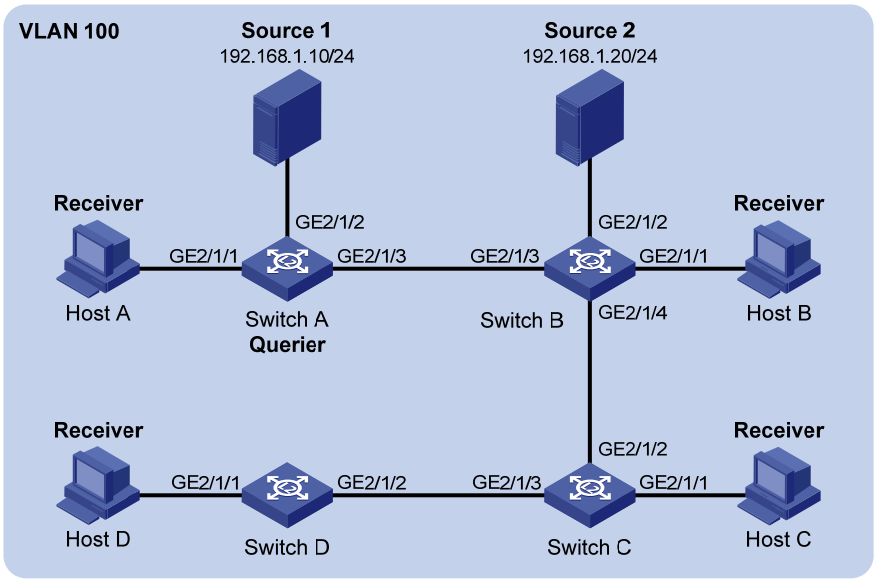
1.9.3 IGMP Snooping查询器配置举例

1. 组网需求

- 如 图 1-5 所示，在一个没有三层设备的纯二层网络环境中，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，在所有交换机上都使能丢弃未知组播数据报文功能。

2. 组网图

图1-5 IGMP Snooping 查询器配置组网图



3. 配置步骤

(1) 配置 Switch A

全局使能 IGMP Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 到 GigabitEthernet2/1/3 添加到该 VLAN 中；在该 VLAN 内使能 IGMP Snooping，并使能丢弃未知组播数据报文功能。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 2/1/1 to gigabitethernet 2/1/3
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping drop-unknown
```

在 VLAN 100 内使能 IGMP Snooping 查询器。

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

(2) 配置 Switch B

全局使能 IGMP Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 到 GigabitEthernet2/1/4 添加到该 VLAN 中；在该 VLAN 内使能 IGMP Snooping，并使能丢弃未知组播数据报文功能。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 2/1/1 to gigabitethernet 2/1/4
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] igmp-snooping drop-unknown
```

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

(3) 配置 Switch C

全局使能 IGMP Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 到 GigabitEthernet2/1/3 添加到该 VLAN 中；在该 VLAN 内使能 IGMP Snooping，并使能丢弃未知组播数据报文功能。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 2/1/1 to gigabitethernet 2/1/3
[SwitchC-vlan100] igmp-snooping enable
[SwitchC-vlan100] igmp-snooping drop-unknown
[SwitchC-vlan100] quit
```

(4) 配置 Switch D

全局使能 IGMP Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 到 GigabitEthernet2/1/2 添加到该 VLAN 中；在该 VLAN 内使能 IGMP Snooping，并使能丢弃未知组播数据报文功能。

```
[SwitchD] vlan 100
[SwitchD-vlan100] port gigabitethernet 2/1/1 to gigabitethernet 2/1/2
[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 error IGMP messages:  0
```

1.10 常见配置错误举例

1.10.1 二层设备不能实现二层组播

1. 故障现象

二层设备不能实现 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** 命令全局使能 IGMP Snooping，然后在 VLAN 视图下使用 **igmp-snooping enable** 命令使能 VLAN 内的 IGMP Snooping。

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

1.10.2 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；
- 没有使能丢弃未知组播数据报文的功能，使得属于过滤策略之外的组播数据报文（即未知组播数据报文）被广播。

3. 处理过程

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

(2) 在 IGMP-Snooping 视图或相应的接口视图下使用 **display this** 命令查看是否应用了正确的组播组策略。如果没有，则使用 **group-policy** 或 **igmp-snooping group-policy** 命令应用正确的组播组策略。

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

目 录

1 组播路由与转发

1.1 组播路由与转发简介

组播路由与转发中有以下三种表：

- 每个组播路由协议都有一个协议自身的路由表，如 PIM 路由表。
- 各组播路由协议的组播路由信息经过综合形成一个总的组播路由表，该表由一系列（S，G）表项组成，即一系列由组播源 S 向组播组 G 发送组播数据的组播路由信息。组播路由表中包含了由一或多种组播路由协议生成的组播路由。
- 组播转发表直接用于控制组播数据包的转发，它与组播路由表保持一致，组播路由表中最优的组播路由会直接下发到组播转发表中。

1.1.1 RPF检查机制

组播路由协议依赖于现有的单播路由信息、MBGP 路由或组播静态路由来创建组播路由表项。组播路由协议在创建组播路由表项时，运用了 RPF（Reverse Path Forwarding，逆向路径转发）检查机制，以确保组播数据能够沿正确的路径传输，同时还能避免由于各种原因而造成的环路。

1. RPF检查过程

执行 RPF 检查的依据是单播路由、MBGP 路由或组播静态路由：

- 单播路由表中汇集了到达各个目的网段的最短路径；
- MBGP 路由表直接提供组播路由信息；
- 组播静态路由表中列出了用户通过手工静态配置指定的 RPF 路由信息。

在执行 RPF 检查时，路由器同时查找单播路由表、MBGP 路由表和组播静态路由表，具体过程如下：

(1) 首先，分别从单播路由表、MBGP 路由表和组播静态路由表中各选出一条最优路由：

- 以“报文源”的 IP 地址为目的地址查找单播路由表，自动选取一条最优单播路由。对应表项中的出接口为 RPF 接口，下一跳为 RPF 邻居。路由器认为来自 RPF 邻居且由该 RPF 接口收到的组播报文所经历的路径是从源 S 到本地的最短路径。
- 以“报文源”的 IP 地址为目的地址查找 MBGP 路由表，自动选取一条最优 MBGP 路由。对应表项中的出接口为 RPF 接口，下一跳为 RPF 邻居。
- 以“报文源”的 IP 地址为指定源地址查找组播静态路由表，自动选取一条最优组播静态路由。对应表项明确指定了 RPF 接口和 RPF 邻居。

(2) 然后，从这三条最优路由中选择一条作为 RPF 路由：

- 如果配置了按照最长匹配选择路由，则从这三条路由中选出最长匹配的那条路由；如果这三条路由的掩码一样，则选择其中路由优先级最高的那条路由；如果它们的路由优先级也相同，则按照组播静态路由、MBGP 路由、单播路由的顺序进行选择。有关路由优先级的详细介绍，请参见“三层技术-IP 路由配置指导”中的“IP 路由基础”。
- 如果没有配置按照最长匹配选择路由，则从这三条路由中选出路由优先级最高的那条路由；如果它们的路由优先级相同，则按照组播静态路由、MBGP 路由、单播路由的顺序进行选择。

说明

根据组播报文传输的具体情况不同，“报文源”所代表的具体含义也不同：

- 如果当前报文沿从组播源到接收者或 RP（Rendezvous Point，汇集点）的 SPT（Shortest Path Tree，最短路径树）进行传输，则以组播源为“报文源”进行 RPF 检查；
- 如果当前报文沿从 RP 到接收者的 RPT（Rendezvous Point Tree，共享树）进行传输，或者沿从组播源到 RP 的组播源侧 RPT 进行传输，则都以 RP 为“报文源”进行 RPF 检查；
- 如果当前报文为 BSR（Bootstrap Router，自举路由器）报文，沿从 BSR 到各路由器的路径进行传输，则以 BSR 为“报文源”进行 RPF 检查。

有关 SPT、RPT、组播源侧 RPT、RP 和 BSR 的详细介绍，请参见“IP 组播配置指导”中的“PIM”。

2. RPF检查在组播转发中的应用

对每一个收到的组播数据报文都进行 RPF 检查会给路由器带来较大负担，而利用组播转发表可以解决这个问题。在建立组播路由和转发表时，会把组播数据报文（S，G）的 RPF 接口记录为（S，G）表项的入接口。当路由器收到组播数据报文（S，G）后，查找组播转发表：

(1) 如果组播转发表中不存在（S，G）表项，则对该报文执行 RPF 检查，将其 RPF 接口作为入接口，结合相关路由信息创建相应的表项，并下发到组播转发表中：

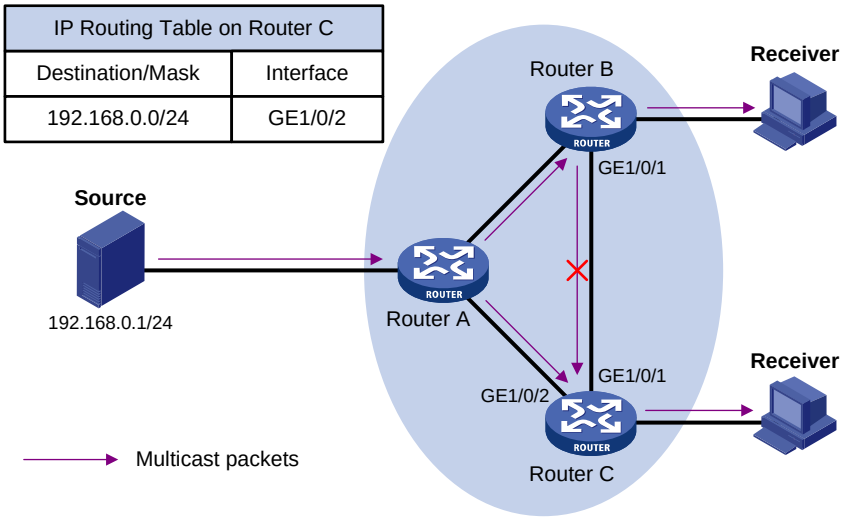
- 若该报文实际到达的接口正是其 RPF 接口，则 RPF 检查通过，向所有的出接口转发该报文；
- 若该报文实际到达的接口不是其 RPF 接口，则 RPF 检查失败，丢弃该报文。

(2) 如果组播转发表中已存在（S，G）表项，且该报文实际到达的接口与入接口相匹配，则向所有的出接口转发该报文。

(3) 如果组播转发表中已存在（S，G）表项，但该报文实际到达的接口与入接口不匹配，则对此报文执行 RPF 检查：

- 若其 RPF 接口与入接口一致，则说明（S，G）表项正确，丢弃这个来自错误路径的报文；
- 若其 RPF 接口与入接口不符，则说明（S，G）表项已过时，于是把入接口更新为 RPF 接口。如果该报文实际到达的接口正是其 RPF 接口，则向所有的出接口转发该报文，否则将其丢弃。

图1-1 RPF 检查过程



如 图 1-1 所示，假设网络中单播路由畅通，未配置MBGP，Router C上也未配置组播静态路由。组播报文（S，G）沿从组播源（Source）到接收者（Receiver）的SPT进行传输。假定Router C上的组播转发表中已存在（S，G）表项，其记录的入接口为GigabitEthernet1/0/2：

- 如果该组播报文从接口 GigabitEthernet1/0/2 到达 Router C，与（S，G）表项的入接口相匹配，则向所有的出接口转发该报文。
- 如果该组播报文从接口 GigabitEthernet1/0/1 到达 Router C，与（S，G）表项的入接口不匹配，则对其执行 RPF 检查：通过查找单播路由表发现到达 Source 的出接口（即 RPF 接口）是 GigabitEthernet1/0/2，与（S，G）表项的入接口一致。这说明（S，G）表项是正确的，该报文来自错误的路径，RPF 检查失败，于是丢弃该报文。

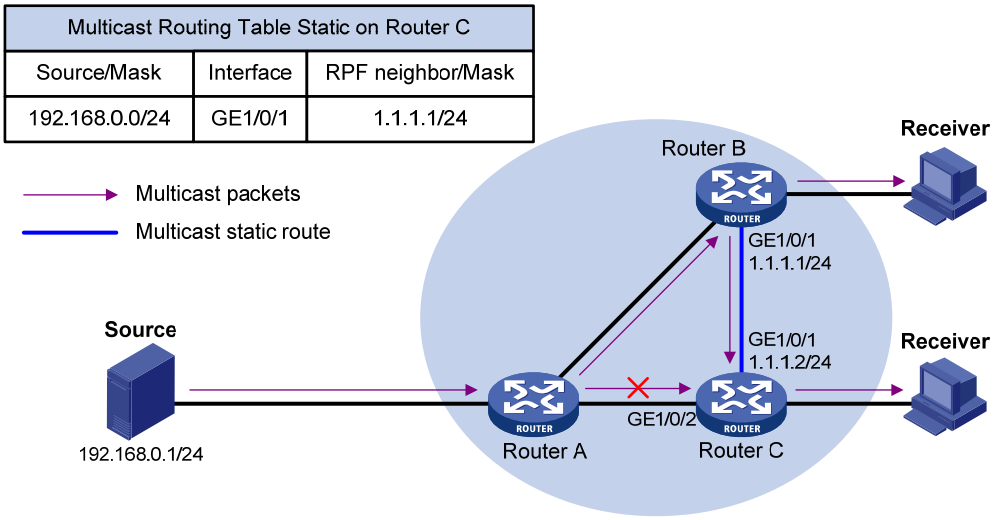
1.1.2 组播静态路由

根据具体应用环境的不同，组播静态路由有以下两种主要用途：

1. 改变RPF路由

通常，组播的网络拓扑结构与单播相同，组播数据的传输路径也与单播相同。可以通过配置组播静态路由以改变 RPF 路由，从而为组播数据创建一条与单播不同的传输路径。

图1-2 改变 RPF 路由示意图

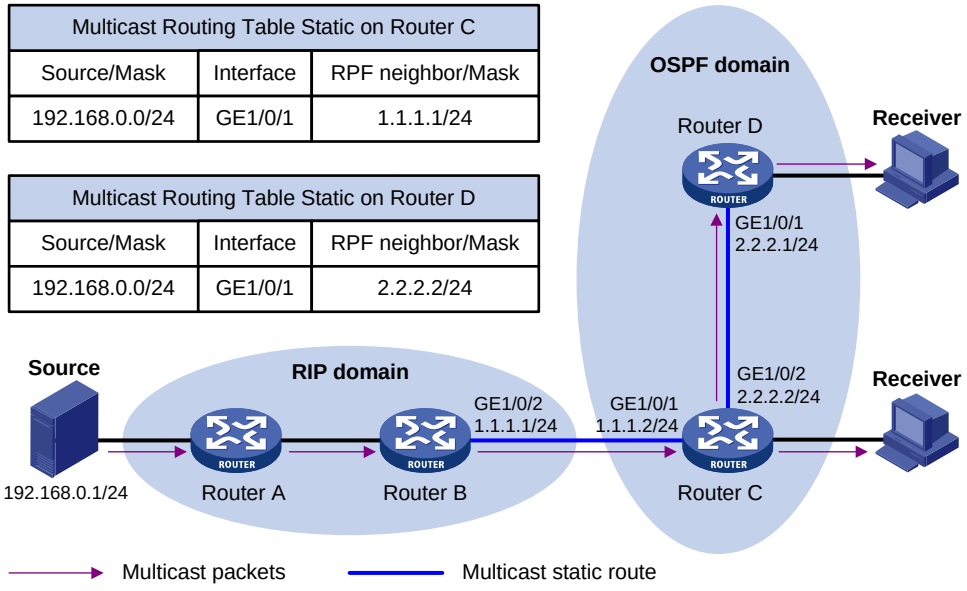


如 图 1-2 所示，当网络中没有配置组播静态路由时，Router C到组播源（Source）的RPF邻居为Router A，从Source发出的组播信息沿Router A—Router C的路径传输，与单播路径一致；当在Router C上配置了组播静态路由，指定从Router C到Source的RPF邻居为Router B之后，从Source发出的组播信息将改变传输路径，沿Router A—Router B—Router C的新路径传输。

2. 衔接RPF路由

当网络中的单播路由被阻断时，由于没有 RPF 路由而无法进行包括组播数据在内的数据转发。可以通过配置组播静态路由以生成 RPF 路由，从而创建组播路由表项以指导组播数据的转发。

图1-3 衔接 RPF 路由示意图



如 图 1-3 所示，RIP域与OSPF域之间实行单播路由隔离。当网络中没有配置组播静态路由时，OSPF域内的接收者（Receiver）不能收到RIP域内的组播源（Source）所发出的组播信息；当在Router C

和Router D上均配置了组播静态路由，分别指定从Router C到Source的RPF邻居为Router B、从Router D到Source的RPF邻居为Router C之后，Receiver便能收到Source发出的组播信息了。

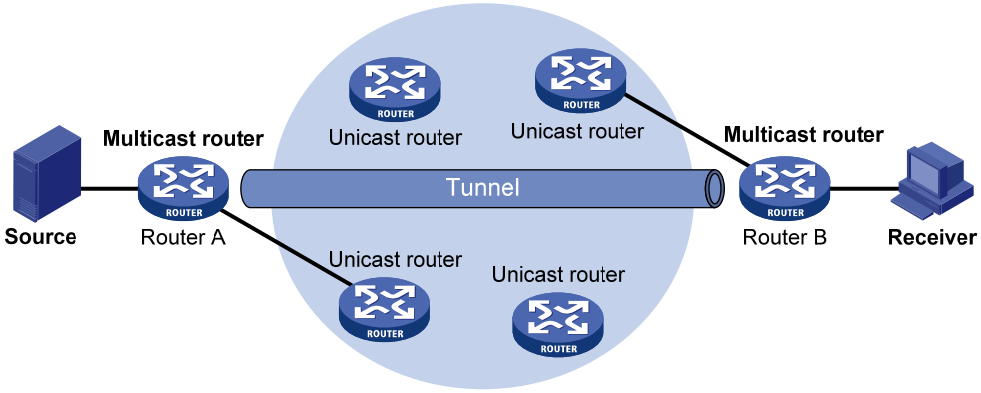
说明

组播静态路由仅在所配置的组播路由器上生效，不会以任何方式被广播或者引入给其它路由器。

1.1.3 跨单播网段的组播转发

网络中可能存在不支持组播协议的路由器，从组播源发出的组播数据沿组播路由器逐跳转发，当下一跳路由器不支持组播协议时，组播转发路径将被阻断。而通过在处于单播网段两端的组播路由器之间建立隧道，则可以实现跨单播网段的组播数据转发。

图1-4 使用隧道传输组播数据



如 图 1-4 所示，在组播路由器Router A和Router B之间建立隧道。Router A将组播数据封装在单播报文中，通过单播路由器转发至隧道另一端的Router B，再由Router B将单播报文头剥掉后继续进行组播传输。

若要将该隧道专用于组播数据传输，可以在隧道两端只配置组播静态路由而不配置单播静态路由，从而使单播数据报文无法利用此隧道进行传输。

1.2 组播路由与转发配置任务简介

表1-1 组播路由与转发配置任务简介

配置任务		说明	详细配置
使能IP组播路由		必选	1.3
配置组播路由与转发	配置组播静态路由	可选	1.4.2
	配置按照最长匹配选择RPF路由	可选	1.4.3
	配置对组播流量进行负载分担	可选	1.4.4
	配置组播转发边界	可选	1.4.5

说明

当一个接口配置有从 IP 地址或借用了其它接口的 IP 地址时，组播数据并不能通过从 IP 地址或借来的 IP 地址进行路由和转发，而只能通过该接口的主 IP 地址进行路由与转发。有关主、从 IP 地址以及 IP 地址借用的详细介绍，请参见“三层技术-IP 业务配置指导”中的“IP 地址”。

1.3 使能IP组播路由

在公网实例或 VPN 实例中配置各项三层组播功能之前，必须先在该实例中使能 IP 组播路由。

表1-2 使能 IP 组播路由

操作	命令	说明
进入系统视图	**system-view**	-
使能IP组播路由，并进入MRIB（Multicast Routing Information Base，组播路由信息库）视图	**multicast routing** [**vpn-instance** *vpn-instance-name*]	缺省情况下，IP组播路由处于关闭状态

1.4 配置组播路由与转发

1.4.1 配置准备

在配置组播路由与转发之前，需完成以下任务：

- 配置任一单播路由协议，实现域内网络层互通
- 配置 PIM-DM 或 PIM-SM

1.4.2 配置组播静态路由

通过配置组播静态路由，可以为来自特定组播源的组播报文指定 RPF 接口或 RPF 邻居。在删除已配置好的组播静态路由时，除了可以通过 **undo ip rpf-route-static** 命令删除指定的组播静态路由外，还可以通过 **delete ip rpf-route-static** 命令删除所有的组播静态路由。

表1-3 配置组播静态路由

操作	命令	说明
进入系统视图	**system-view**	-
配置组播静态路由	**ip rpf-route-static** [**vpn-instance** *vpn-instance-name*] *source-address* { *mask-length* | *mask* } { *rpf-nbr-address* | *interface-type interface-number* } [**preference** *preference*]	缺省情况下，不存在任何组播静态路由
（可选）删除所有组播静态路由	**delete ip rpf-route-static** [**vpn-instance** *vpn-instance-name*]	-

1.4.3 配置按照最长匹配选择RPF路由

用户可以配置组播路由器按照最长匹配原则来选择RPF路由，有关RPF路由选择的详细介绍，请参见“1.1.1 1. RPF检查过程”一节。

表1-4 配置按照最长匹配选择 RPF 路由

操作	命令	说明
进入系统视图	**system-view**	-
进入MRIB视图	**multicast routing** [**vpn-instance** *vpn-instance-name*]	-
配置按照最长匹配选择RPF路由	**longest-match**	缺省情况下，选择路由优先级最高的路由作为RPF路由

1.4.4 配置对组播流量进行负载分担

用户通过配置根据组播源或组播源组进行组播流量的负载分担，可以优化存在多条组播数据流时的网络流量。

表1-5 配置对组播流量进行负载分担

操作	命令	说明
进入系统视图	**system-view**	-
进入MRIB视图	**multicast routing** [**vpn-instance** *vpn-instance-name*]	-
配置对组播流量进行负载分担	**load-splitting** { **source** | **source-group** }	缺省情况下，不对组播流量进行负载分担

1.4.5 配置组播转发边界

提示

进行本配置不需要使能 IP 组播路由。

组播信息在网络中的转发并不是漫无边际的，每个组播组对应的组播信息都必须在确定的范围内传递。组播转发边界为指定范围的组播组划定了边界条件，如果组播报文的目的地址与边界条件匹配，就停止转发。当在一个接口上配置了组播转发边界后，将不能从该接口转发组播报文（包括本机发出的组播报文），也不能从该接口接收组播报文。

表1-6 配置组播转发边界

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
配置组播转发边界	**multicast boundary** *group-address* { *mask-length* | *mask* }	缺省情况下，没有配置组播转发边界

1.5 组播路由与转发显示和维护

注意

执行 **reset** 命令清除组播路由表或组播转发表中的信息，可能导致组播信息无法正常传输。

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路由与转发的信息，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除组播路由与转发的统计信息。

表1-7 组播路由与转发显示和维护

操作	命令
显示MRIB维护的接口信息	**display mrib** [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*]
显示组播边界的信息	**display multicast** [**vpn-instance** *vpn-instance-name*] **boundary** [*group-address* [*mask-length* | *mask*]] [**interface** *interface-type interface-number*]
显示组播转发的DF信息（MSR 2600/MSR 3600）	**display multicast** [**vpn-instance** *vpn-instance-name*] **forwarding df-info** [*rp-address*] [**verbose**]
显示组播转发的DF信息（MSR 5600）	**display multicast** [**vpn-instance** *vpn-instance-name*] **forwarding df-info** [*rp-address*] [**verbose**] [**slot** *slot-number*]
显示组播转发的事件统计信息（MSR 2600/MSR 3600）	**display multicast** [**vpn-instance** *vpn-instance-name*] **forwarding event**
显示组播转发的事件统计信息（MSR 5600）	**display multicast** [**vpn-instance** *vpn-instance-name*] **forwarding event** [**slot** *slot-number*]
显示组播转发表的信息（MSR 2600/MSR 3600）	**display multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number* | **statistics**] *
显示组播转发表的信息（MSR 5600）	**display multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number* | **slot** *slot-number* | **statistics**] *
显示组播转发表的DF列表信息（MSR 2600/MSR 3600）	**display multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table df-list** [*group-address*] [**verbose**]
显示组播转发表的DF列表信息（MSR 5600）	**display multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table df-list** [*group-address*] [**verbose**] [**slot** *slot-number*]

操作	命令
显示组播路由表的信息	**display multicast** [**vpn-instance** *vpn-instance-name*] **routing-table** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *
显示组播静态路由表的信息	**display multicast** [**vpn-instance** *vpn-instance-name*] **routing-table static** [*source-address* { *mask-length* | *mask* }]
显示组播源的RPF信息	**display multicast** [**vpn-instance** *vpn-instance-name*] **rpf-info** *source-address* [*group-address*]
清除组播转发的事件统计信息	**reset multicast** [**vpn-instance** *vpn-instance-name*] **forwarding event**
清除组播转发表中的转发项	**reset multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table** { { *source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** { *interface-type interface-number* } } * | **all** }
清除组播路由表中的路由项	**reset multicast** [**vpn-instance** *vpn-instance-name*] **routing-table** { { *source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** *interface-type interface-number* } * | **all** }

说明

- 清除组播路由表中的路由项后，组播转发表中的相应表项也将随之删除。
- 清除组播转发表中的转发项后，组播路由表中的相应表项也将随之删除。

1.6 组播路由与转发典型配置举例

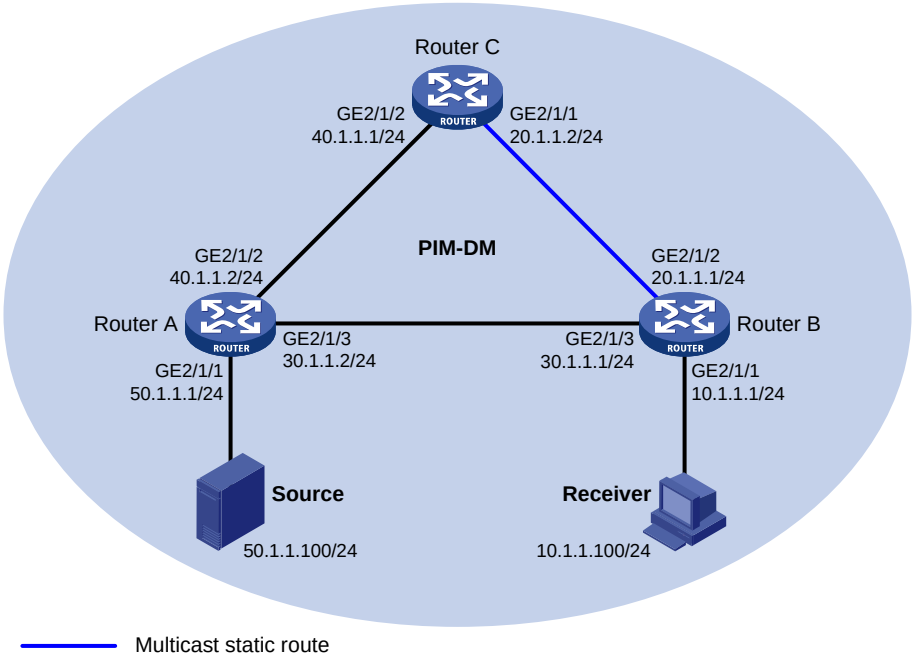
1.6.1 改变RPF路由配置举例

1. 组网需求

- 网络中运行 PIM-DM，所有路由器都支持组播功能；
- Router A、Router B 和 Router C 之间运行 OSPF 协议；
- 通常情况下，Receiver 能通过 Router A—Router B 这条与单播路径相同的路径接收来自 Source 的组播信息；
- 要求通过配置，使 Receiver 能通过 Router A—Router C—Router B 这条与单播路径不同的路径接收来自 Source 的组播信息。

2. 组网图

图1-5 改变 RPF 路由配置举例



3. 配置步骤

(1) 配置 IP 地址和单播路由协议

请按照 图 1-5 配置各接口的IP地址和掩码，具体配置过程略。

配置 PIM-DM 域内的各路由器之间采用 OSPF 协议进行互连，确保 PIM-DM 域内部在网络层互通，并且各路由器之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，并使能 PIM-DM 和 IGMP

在 Router B 上使能 IP 组播路由，在主机侧接口 GigabitEthernet2/1/1 上使能 IGMP，并在其它接口上使能 PIM-DM。

```
<RouterB> system-view
[RouterB] multicast routing
[RouterB-mrib] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] igmp enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] pim dm
[RouterB-GigabitEthernet2/1/2] quit
[RouterB] interface gigabitethernet 2/1/3
[RouterB-GigabitEthernet2/1/3] pim dm
[RouterB-GigabitEthernet2/1/3] quit
```

在 Router A 上使能 IP 组播路由，并在各接口上使能 PIM-DM。

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

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] pim dm
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] pim dm
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] interface gigabitethernet 2/1/3
[RouterA-GigabitEthernet2/1/3] pim dm
[RouterA-GigabitEthernet2/1/3] quit
```

Router C 上的配置与 Router A 相似，配置过程略。

在 Router B 上使用 **display multicast rpf-info** 命令查看到 Source 的 RPF 信息。

```
[RouterB] display multicast rpf-info 50.1.1.100
 RPF information about source 50.1.1.100:
     RPF interface: GigabitEthernet2/1/3, RPF neighbor: 30.1.1.2
     Referenced route/mask: 50.1.1.0/24
     Referenced route type: igp
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

Router B 上当前的 RPF 路由来源于单播路由，RPF 邻居是 Router A。

(3) 配置组播静态路由

在 Router B 上配置组播静态路由，指定到 Source 的 RPF 邻居为 Router C。

```
[RouterB] ip rpf-route-static 50.1.1.100 24 20.1.1.2
```

在 Router B 上使用 **display multicast rpf-info** 命令查看到 Source 的 RPF 信息。

```
[RouterB] display multicast rpf-info 50.1.1.100
 RPF information about source 50.1.1.100:
     RPF interface: GigabitEthernet2/1/2, RPF neighbor: 20.1.1.2
     Referenced route/mask: 50.1.1.0/24
     Referenced route type: multicast static
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

与配置组播静态路由前相比，Router B 上的 RPF 路由已经产生了变化，其来源变为组播静态路由，RPF 邻居变为 Router C。

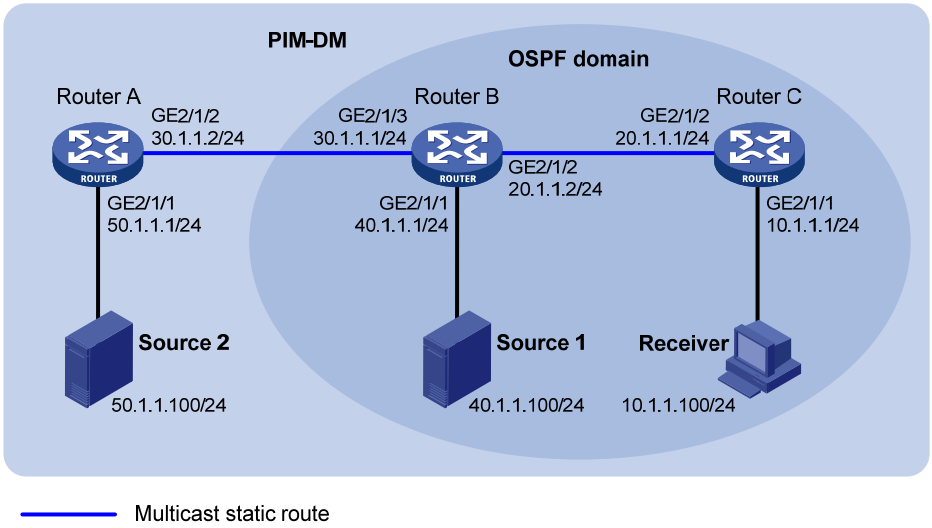
1.6.2 衔接RPF路由配置举例

1. 组网需求

- 网络中运行 PIM-DM，所有路由器都支持组播功能；
- Router B 和 Router C 之间运行 OSPF 协议，并与 Router A 单播路由隔离；
- 通常情况下，Receiver 能接收来自 OSPF 域内 Source 1 的组播信息；
- 要求通过配置，使 Receiver 也可以接收来自 OSPF 域外 Source 2 的组播信息。

2. 组网图

图1-6 衔接 RPF 路由配置组网图



3. 配置步骤

(1) 配置 IP 地址和单播路由协议

请按照 图 1-6 配置各接口的IP地址和掩码，具体配置过程略。

配置 Router B 和 Router C 之间采用 OSPF 协议进行互连，确保 Router B 和 Router C 之间在网络层互通，并且能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，并使能 PIM-DM 和 IGMP

在 Router C 上使能 IP 组播路由，在接口 GigabitEthernet2/1/2 上使能 PIM-DM，并在主机侧接口 GigabitEthernet2/1/1 上使能 IGMP。

```
<RouterC> system-view
[RouterC] multicast routing
[RouterC-mrib] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] igmp enable
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface gigabitethernet 2/1/2
[RouterC-GigabitEthernet2/1/2] pim dm
[RouterC-GigabitEthernet2/1/2] quit
```

在 Router A 上使能 IP 组播路由，并在各接口上使能 PIM-DM。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] pim dm
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] pim dm
[RouterA-GigabitEthernet2/1/2] quit
```

Router B 上的配置与 Router A 相似，配置过程略。

在 Router B 和 Router C 上分别使用 **display multicast rpf-info** 命令查看到 Source 2 的 RPF 信息。

```
[RouterB] display multicast rpf-info 50.1.1.100
[RouterC] display multicast rpf-info 50.1.1.100
```

没有显示信息输出，说明在 Router B 和 Router C 上都没有到 Source 2 的 RPF 路由。

(3) 配置组播静态路由

在 Router B 上配置组播静态路由，指定到 Source 2 的 RPF 邻居为 Router A。

```
[RouterB] ip rpf-route-static 50.1.1.100 24 30.1.1.2
```

在 Router C 上配置组播静态路由，指定到 Source 2 的 RPF 邻居为 Router B。

```
[RouterC] ip rpf-route-static 50.1.1.100 24 20.1.1.2
```

4. 验证配置

在 Router B 和 Router C 上分别使用 **display multicast rpf-info** 命令查看到 Source 2 的 RPF 信息。

```
[RouterB] display multicast rpf-info 50.1.1.100
 RPF information about source 50.1.1.100:
     RPF interface: GigabitEthernet2/1/3, RPF neighbor: 30.1.1.2
     Referenced route/mask: 50.1.1.0/24
     Referenced route type: multicast static
     Route selection rule: preference-preferred
     Load splitting rule: disable
[RouterC] display multicast rpf-info 50.1.1.100
 RPF information about source 50.1.1.100:
     RPF interface: GigabitEthernet2/1/2, RPF neighbor: 20.1.1.2
     Referenced route/mask: 50.1.1.0/24
     Referenced route type: multicast static
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

与配置组播静态路由前相比，Router B 和 Router C 上都有了到 Source 2 的 RPF 路由，且其均来源于组播静态路由。

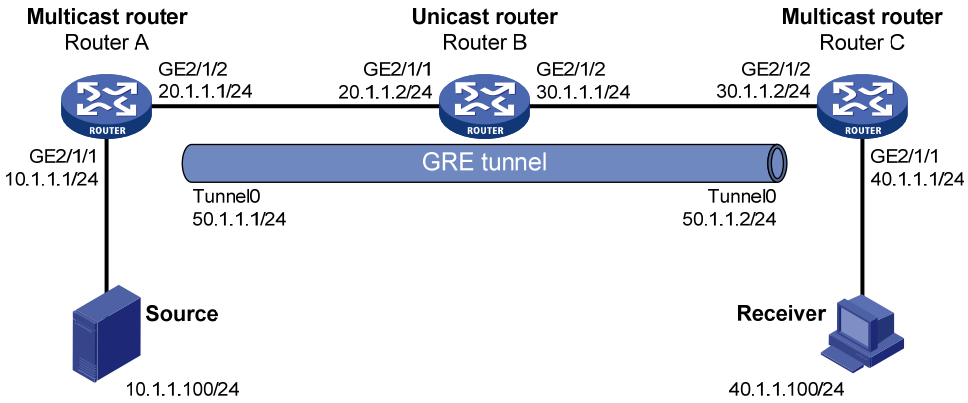
1.6.3 利用GRE隧道实现组播转发配置举例

1. 组网需求

- Router A 和 Router C 支持组播功能并运行 PIM-DM，但 Router B 不支持组播功能；
- Router A、Router B 和 Router C 之间运行 OSPF 协议；
- 要求通过配置，使 Receiver 能够接收来自 Source 的组播信息。

2. 组网图

图1-7 利用 GRE 隧道实现组播转发配置组网图



3. 配置步骤

(1) 配置 IP 地址和单播路由协议

请按照 图 1-7 配置各接口的IP地址和掩码，具体配置过程略。

配置各路由器之间采用 OSPF 协议进行互连，确保各路由器之间在网络层互通，并能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 配置 GRE 隧道

在 Router A 上创建接口 Tunnel0，并指定其隧道模式为 GRE over IPv4 隧道。

```
<RouterA> system-view
[RouterA] interface tunnel 0 mode gre
```

在 Router A 上为 Tunnel0 接口配置 IP 地址，并指定隧道的源地址和目的地址。

```
[RouterA-Tunnel0] ip address 50.1.1.1 24
[RouterA-Tunnel0] source 20.1.1.1
[RouterA-Tunnel0] destination 30.1.1.2
[RouterA-Tunnel0] quit
```

在 Router C 上创建接口 Tunnel0，并指定其隧道模式为 GRE over IPv4 隧道。

```
<RouterC> system-view
[RouterC] interface tunnel 0 mode gre
```

在 Router C 上为 Tunnel0 接口配置 IP 地址，并指定隧道的源地址和目的地址。

```
[RouterC-Tunnel0] ip address 50.1.1.2 24
[RouterC-Tunnel0] source 30.1.1.2
[RouterC-Tunnel0] destination 20.1.1.1
[RouterC-Tunnel0] quit
[RouterC-ospf-1] quit
```

(3) 使能 IP 组播路由，并使能 PIM-DM 和 IGMP

在 Router A 上使能 IP 组播路由，并在各接口上使能 PIM-DM。

```
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] pim dm
```

```
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] pim dm
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] interface tunnel 0
[RouterA-Tunnel0] pim dm
[RouterA-Tunnel0] quit
```

在 Router C 上使能 IP 组播路由，在主机侧接口 GigabitEthernet2/1/1 上使能 IGMP，并在其它接口上使能 PIM-DM。

```
[RouterC] multicast routing
[RouterC-mrib] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] igmp enable
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface gigabitethernet 2/1/2
[RouterC-GigabitEthernet2/1/2] pim dm
[RouterC-GigabitEthernet2/1/2] quit
[RouterC] interface tunnel 0
[RouterC-Tunnel0] pim dm
[RouterC-Tunnel0] quit
```

(4) 配置组播静态路由

在 Router C 上配置组播静态路由，指定到 Source 的 RPF 邻居为 Router A 的 Tunnel0 接口。

```
[RouterC] ip rpf-route-static 10.1.1.0 24 50.1.1.1
```

4. 验证配置

组播源向组播组 225.1.1.1 发送组播数据，接收者加入该组播组后能够收到组播源发来的组播数据。通过使用 **display pim routing-table** 命令可以查看路由器的 PIM 路由表信息。例如：

显示 Router C 上的 PIM 路由表信息。

```
[RouterC] display pim routing-table
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 225.1.1.1)
     Protocol: pim-dm, Flag: WC
     UpTime: 00:04:25
     Upstream interface: NULL
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/1/1
             Protocol: igmp, UpTime: 00:04:25, Expires: -

 (10.1.1.100, 225.1.1.1)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:06:14
     Upstream interface: Tunnel0
         Upstream neighbor: 50.1.1.1
```

```
    RPF prime neighbor: 50.1.1.1
Downstream interface(s) information:
Total number of downstreams: 1
    1: GigabitEthernet2/1/1
        Protocol: pim-dm, UpTime: 00:04:25, Expires: -
```

Router C 的 RPF 邻居为 Router A，组播数据通过 GRE 隧道由直接 Router A 发往 Router C。

1.7 常见配置错误举例

1.7.1 组播静态路由失败

1. 故障现象

路由器没有配置动态路由协议，接口的物理状态与链路层协议状态都显示为 up；但是组播静态路由失败。

2. 故障分析

- 如果没有正确配置或更新与当前网络情况相匹配的组播静态路由，则组播静态路由表中不存在此路由项；
- 如果查询到有比组播静态路由更优的路由，也可能导致组播静态路由失败。

3. 处理过程

(1) 使用 **display multicast routing-table static** 命令显示组播静态路由表的信息，以确定是否正确配置了对应的路由并存在于组播静态路由表中。

(2) 检查组播静态路由与 RPF 邻居相连接口的接口类型，如果不是点到点接口，则 RPF 邻居必须使用指定地址的形式配置。

目 录

1 IGMP

1.1 IGMP简介

IGMP（Internet Group Management Protocol，互联网组管理协议）用于在三层设备和其直连网段中的用户主机之间建立和维护组播组成员关系。

1.1.1 IGMP的版本

到目前为止，IGMP 有三个版本：

- IGMPv1（由 RFC 1112 定义）
- IGMPv2（由 RFC 2236 定义）
- IGMPv3（由 RFC 3376 定义）

所有版本的 IGMP 都支持 ASM（Any-Source Multicast，任意信源组播）模型；IGMPv3 可以直接应用于 SSM（Source-Specific Multicast，指定信源组播）模型，而 IGMPv1 和 IGMPv2 则需要在 IGMP SSM Mapping 技术的支持下才能应用于 SSM 模型。有关 ASM 和 SSM 模型的介绍，请参见“IP 组播配置指导”中的“组播概述”。

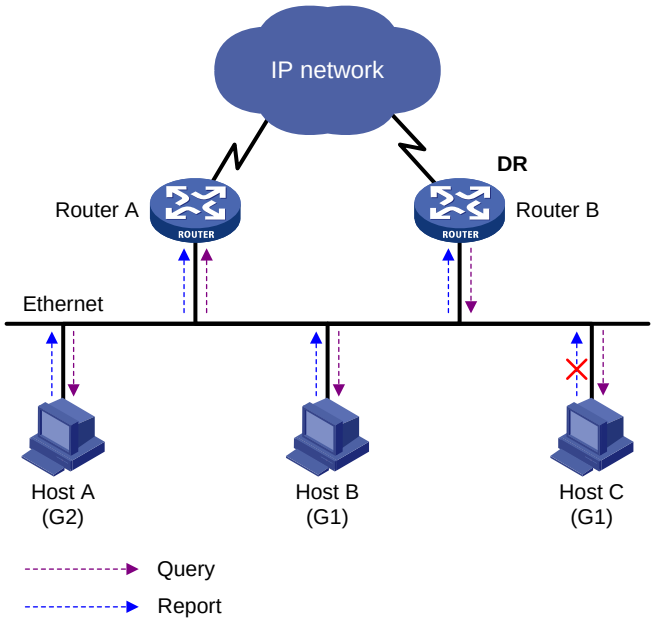
1.1.2 IGMPv1 工作机制

IGMPv1 主要基于查询和响应机制来完成对组播组成员的管理。

当一个网段内有多台运行 IGMP 的路由器时，由于它们都能从主机那里收到 IGMP 成员关系报告报文（Membership Report Message），因此只需其中一台路由器发送 IGMP 查询报文（Query Message）即可，该路由器就称为 IGMP 查询器（Querier）。这就需要有一个查询器的选举机制来确定由哪台路由器作为 IGMP 查询器。

对于 IGMPv1 来说，由组播路由协议（如 PIM）选举出唯一的组播信息转发者 DR（Designated Router，指定路由器）作为 IGMP 查询器。有关 DR 的介绍，请参见“IP 组播配置指导”中的“PIM”。

图1-1 IGMP 查询响应示意图



如 图 1-1 所示，假设Host B与Host C想要收到发往组播组G1 的组播数据，而Host A想要收到发往组播组G2 的组播数据，那么主机加入组播组以及IGMP查询器（Router B）维护组播组成员关系的基本过程如下：

(1) 主机会主动向其要加入的组播组发送 IGMP 成员关系报告报文以声明加入，而不必等待 IGMP 查询器发来的 IGMP 查询报文；

(2) IGMP 查询器周期性地以组播方式向本地网段内的所有主机与路由器发送 IGMP 查询报文（目的地址为 224.0.0.1）；

(3) 在收到该查询报文后，关注 G1 的 Host B 与 Host C 其中之一（这取决于谁的延迟定时器先超时）——譬如 Host B 会首先以组播方式向 G1 发送 IGMP 成员关系报告报文，以宣告其属于 G1。由于本地网段中的所有主机和路由器都能收到 Host B 发往 G1 的报告报文，因此当 Host C 收到该报告报文后，将不再发送同样针对 G1 的报告报文，因为 IGMP 路由器（Router A 和 Router B）已知道本地网段中有对 G1 感兴趣的主机了。这个机制称为主机上的 IGMP 成员关系报告抑制机制，该机制有助于减少本地网段的信息流量；

(4) 与此同时，由于 Host A 关注的是 G2，所以它仍将以组播方式向 G2 发送报告报文，以宣告其属于 G2；

(5) 经过以上的查询和响应过程，IGMP 路由器了解到本地网段中有 G1 和 G2 的成员，于是由组播路由协议（如 PIM）生成（*，G1）和（*，G2）组播转发项作为组播数据的转发依据，其中的“*”代表任意组播源；

(6) 当由组播源发往 G1 或 G2 的组播数据经过组播路由到达 IGMP 路由器时，由于 IGMP 路由器上存在（*，G1）和（*，G2）组播转发项，于是将该组播数据转发到本地网段，接收者主机便能收到该组播数据了。

IGMPv1 没有专门定义离开组播组的报文。当运行 IGMPv1 的主机离开某组播组时，将不会向该组播组发送报告报文。当一个网段中不再有该组播组的成员后，IGMP 路由器将不会收到任何发往该组播组的报告报文，于是在一段时间之后便删除该组播组的记录。

说明

SIC-4FSW/4FSWP 和 SIC-9FSW/9FSWP 交换卡不支持 IGMP 成员关系报告抑制机制。

1.1.3 IGMPv2 的改进

IGMPv2 在兼容和继承 IGMPv1 的基础上，增加了查询器选举机制和离开组播组机制。

1. 查询器选举机制

在 IGMPv1 中，当一个网段内有多台运行 IGMP 的路由器时，由组播路由协议（如 PIM）选举的指定路由器充当查询器。在 IGMPv2 中增加了独立的查询器选举机制，其选举过程如下：

(1) 所有 IGMPv2 路由器在初始时都认为自己是查询器，并向本地网段内的所有主机和路由器发送 IGMP 普遍组查询（General Query）报文（目的地址为 224.0.0.1）；

(2) 本地网段中的其它 IGMPv2 路由器在收到该报文后，将报文的源 IP 地址与自己的接口地址作比较。通过比较，IP 地址最小的路由器将成为查询器，其它路由器成为非查询器（Non-Querier）；

(3) 所有非查询器上都会启动一个定时器（即其它查询器存在时间定时器 Other Querier Present Timer）。在该定时器超时前，如果收到了来自查询器的 IGMP 查询报文，则重置该定时器；否则，就认为原查询器失效，并发起新的查询器选举过程。

2. 离开组播组机制

在 IGMPv1 中，主机离开组播组时不会向组播路由器发出任何通知，导致组播路由器只能依靠组播组成员查询的响应超时来获知组播组成员的离开。而在 IGMPv2 中，当一个主机离开某组播组时：

(1) 该主机向本地网段内的所有组播路由器（目的地址为 224.0.0.2）发送离开组（Leave Group）报文；

(2) 当查询器收到该报文后，向该主机所声明要离开的那个组播组发送特定组查询（Group-Specific Query）报文（目的地址字段和组地址字段均填充为所要查询的组播组地址）；

(3) 如果该网段内还有该组播组的其它成员，则这些成员在收到特定组查询报文后，会在该报文中所设定的最大响应时间（Max Response Time）内发送成员关系报告报文；

(4) 如果在最大响应时间内收到了该组播组其它成员发送的成员关系报告报文，查询器就会继续维护该组播组的成员关系；否则，查询器将认为该网段内已无该组播组的成员，于是不再维护这个组播组的成员关系。

1.1.4 IGMPv3 的改进

IGMPv3 在兼容和继承 IGMPv1 和 IGMPv2 的基础上，进一步增强了主机的控制能力，并增强了查询和报告报文的功能。

1. 主机控制能力的增强

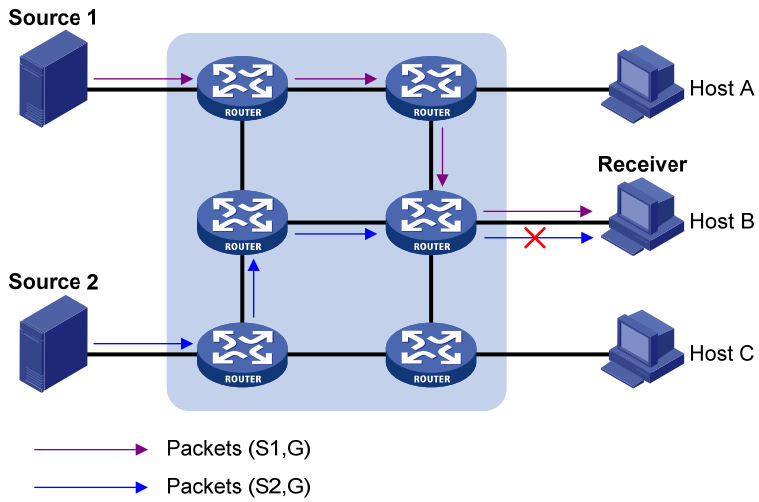
IGMPv3 增加了针对组播源的过滤模式（INCLUDE/EXCLUDE），使主机在加入某组播组 G 的同时，能够明确要求接收或拒绝来自某特定组播源 S 的组播信息。当主机加入组播组时：

- 若要求只接收来自指定组播源如 S1、S2、……的组播信息，则其报告报文中可以标记为 INCLUDE Sources（S1，S2，……）；

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

如 图 1-2 所示，网络中存在Source 1（S1）和Source 2（S2）两个组播源，均向组播组G发送组播报文。Host B仅对从Source 1 发往G的信息感兴趣，而对来自Source 2 的信息没有兴趣。

图1-2 指定源组的组播流路经



如果主机与路由器之间运行的是 IGMPv1 或 IGMPv2，Host B 加入组播组 G 时无法对组播源进行选择，因此无论 Host B 是否需要，来自 Source 1 和 Source 2 的组播信息都将传递给 Host B。

当主机与路由器之间运行了 IGMPv3 之后，Host B 就可以要求只接收来自 Source 1、发往 G 的组播信息（S1，G），或要求拒绝来自 Source 2、发往 G 的组播信息（S2，G），这样就只有来自 Source 1 的组播信息才能传递给 Host B 了。

2. 查询和报告报文功能的增强

(1) 携带源地址的查询报文

IGMPv3 不仅支持 IGMPv1 的普遍组查询和 IGMPv2 的特定组查询，而且还增加了对特定源组查询的支持：

- 普遍组查询报文中，既不携带组地址，也不携带源地址；
- 特定组查询报文中，携带组地址，但不携带源地址；
- 特定源组查询报文中，既携带组地址，还携带一个或多个源地址。

(2) 包含多组记录的报告报文

IGMPv3 报告报文的目的地址为 224.0.0.22，可以携带一个或多个组记录。在每个组记录中，包含有组播组地址和组播源地址列表。组记录可以分为多种类型，如下：

- IS_IN：表示组播组与组播源列表之间的过滤模式为 INCLUDE，即只接收从指定组播源列表发往该组播组的组播数据。
- IS_EX：表示组播组与组播源列表之间的过滤模式为 EXCLUDE，即只接收从指定组播源列表之外的组播源发往该组播组的组播数据。
- TO_IN：表示组播组与组播源列表之间的过滤模式由 EXCLUDE 转变为 INCLUDE。
- TO_EX：表示组播组与组播源列表之间的过滤模式由 INCLUDE 转变为 EXCLUDE。

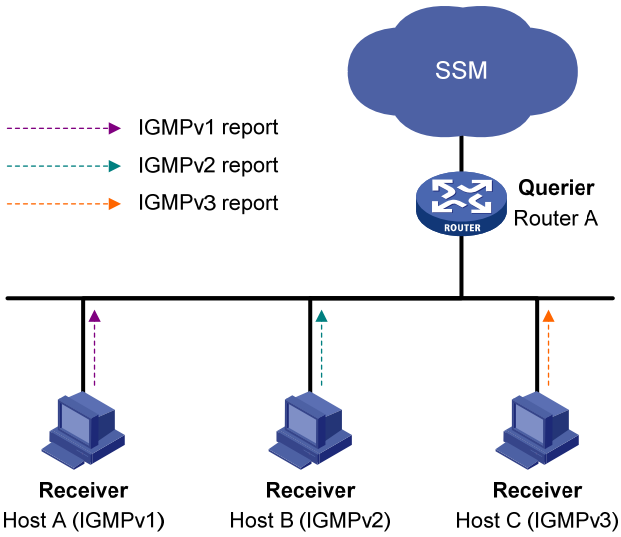
- ALLOW：表示在现有状态的基础上，还希望从某些组播源接收组播数据。如果当前的对应关系为 INCLUDE，则向现有组播源列表中添加这些组播源；如果当前的对应关系为 EXCLUDE，则从现有组播源列表中删除这些组播源。
- BLOCK：表示在现有状态的基础上，不再希望从某些组播源接收组播数据。如果当前的对应关系为 INCLUDE，则从现有组播源列表中删除这些组播源；如果当前的对应关系为 EXCLUDE，则向现有组播源列表中添加这些组播源。

1.1.5 IGMP SSM Mapping

IGMP SSM Mapping 通过在路由器上配置 SSM 静态映射规则，从而为运行 IGMPv1 或 IGMPv2 的接收者主机提供对 SSM 模型的支持。

SSM 模型要求在接收者主机所在的网段，路由器能够了解主机加入组播组时所指定的组播源。如果接收者主机上运行的是 IGMPv3，则可以在 IGMPv3 的报告报文中直接指定组播源的地址；如果某些接收者主机只能运行 IGMPv1 或 IGMPv2，则在 IGMPv1 或 IGMPv2 的报告报文中无法指定组播源的地址。这种情况下需要通过在路由器上配置 IGMP SSM Mapping 规则，将 IGMPv1 或 IGMPv2 报告报文中所包含的（*，G）信息映射为（G，INCLUDE，（S1，S2...））信息。

图1-3 IGMP SSM Mapping 组网图



在如 图 1-3 所示的SSM网络中，Host A、Host B和Host C上分别运行IGMPv1、IGMPv2 和IGMPv3。在不允许将Host A和Host B升级为IGMPv3 的情况下，若要为Host A和Host B也提供SSM组播服务，则需在Router A上配置IGMP SSM Mapping规则。

配置完成后，当 Router A 收到来自主机的 IGMPv1 或 IGMPv2 报告报文时，首先检查该报文中所携带的组播组地址 G，然后根据检查结果的不同分别进行处理：

(1) 如果 G 不在 SSM 组地址范围内，则提供 ASM 组播服务。

(2) 如果 G 在 SSM 组地址范围内：

- 若 Router A 上没有 G 对应的 IGMP SSM Mapping 规则，则无法提供 SSM 组播服务，丢弃该报文；
- 若 Router A 上有 G 对应的 IGMP SSM Mapping 规则，则依据规则将报告报文中所包含的（*，G）信息映射为（G，INCLUDE，（S1，S2...））信息，可以提供 SSM 组播服务。

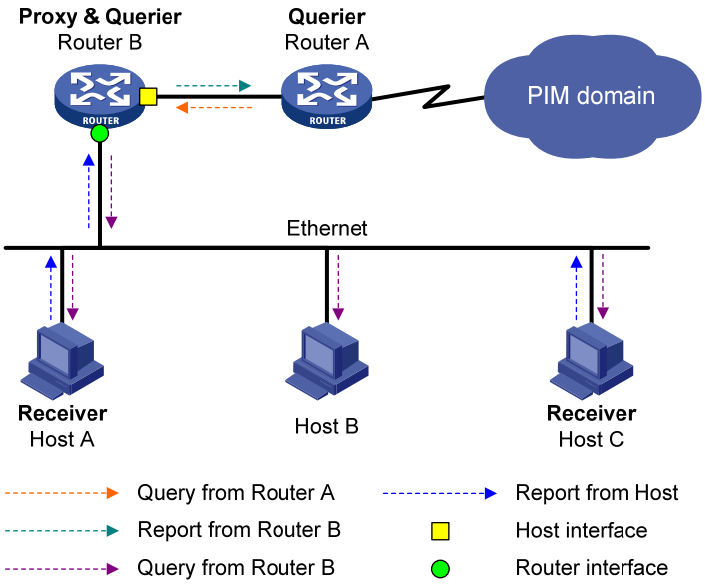
说明

- IGMP SSM Mapping 不对 IGMPv3 的报告报文进行处理。
- 有关 SSM 组地址范围的介绍，请参见“IP 组播配置指导”中的“PIM”。

1.1.6 IGMP代理

在一些简单的树型网络拓扑中，边缘设备上并不需要运行复杂的组播路由协议（如 PIM），可以通过在这些设备上配置 IGMP 代理，使其代理下游主机来发送 IGMP 报文及维护组成员关系，并基于该关系进行组播转发。在上游设备看来，配置了 IGMP 代理功能的设备（称为 IGMP 代理设备）不再是一个 PIM 邻居，而只是一台主机。

图1-4 IGMP 代理组网图



如 图 1-4 所示，IGMP代理中定义了以下两种接口类型：

- 上行接口：又称代理接口，指 IGMP 代理设备上运行 IGMP 代理功能的接口，即朝向组播分发树树根方向的接口。由于该接口执行 IGMP 协议的主机行为，因此也称为主机接口（Host Interface）。
- 下行接口：指 IGMP 代理设备上除上行接口外其它运行 IGMP 协议的接口，即背向组播分发树树根方向的接口。由于该接口执行 IGMP 协议的路由器行为，因此也称为路由器接口（Router Interface）。

IGMP 代理设备上维护着一个组成员关系数据库（Membership Database），将所有下行接口维护的组成员关系记录都存到这个数据库中。组成员关系记录的结构如下：（Multicast-address，Filter-mode，Source-list），每条记录都是各下行接口上具有相同组地址的成员关系记录的合集。

上行接口正是依据这个数据库来执行主机行为——当收到查询报文时根据当前数据库状态响应报告报文，或者当数据库变化时主动发送报告或离开报文；而下行接口则执行路由器行为——参与查询器的选举、发送查询报文并根据报告报文维护组成员关系等。

1.1.7 多实例的IGMP

IGMP 依据接口来维护组成员关系，各实例的 IGMP 根据接口所属的实例来处理协议报文的收发。当路由器收到 IGMP 报文时，需要区分该报文所属的实例，并在该实例范围内对其进行处理。当某实例内的 IGMP 需要和其它组播协议交互信息时，只会通知本实例内的其它组播协议。

1.1.8 协议规范

与 IGMP 相关的协议规范有：

- RFC 1112：Host Extensions for IP Multicasting
- RFC 2236：Internet Group Management Protocol, Version 2
- RFC 3376：Internet Group Management Protocol, Version 3

1.2 IGMP配置任务简介

表1-1 IGMP 配置任务简介

配置任务		说明	详细配置
配置IGMP基本功能	使能IGMP	必选	1.3.2
	配置IGMP版本	可选	1.3.3
	配置静态加入	可选	1.3.4
	配置组播组过滤器	可选	1.3.5
调整IGMP性能	配置IGMP查询	可选	1.4.2
	配置组播组成员快速离开	可选	1.4.3
配置IGMP SSM Mapping		可选	1.5.2
配置IGMP代理	使能IGMP代理功能	可选	1.6.2
	配置非查询器转发功能	可选	1.6.3
	配置IGMP代理的负载分担功能	可选	1.6.4

1.3 配置IGMP基本功能

1.3.1 配置准备

在配置 IGMP 基本功能之前，需完成以下任务：

- 配置任一单播路由协议，实现网络层互通
- 配置 PIM 协议

在配置 IGMP 基本功能之前，需准备以下数据：

- IGMP 的版本
- 以静态方式加入的组播组和组播源的地址
- 组播组过滤的 ACL 规则

1.3.2 使能IGMP

在需要建立和维护组播组成员关系的接口上使能 IGMP。

表1-2 使能 IGMP

操作	命令	说明
进入系统视图	**system-view**	-
使能IP组播路由，并进入MRIB视图	**multicast routing** [**vpn-instance** *vpn-instance-name*]	缺省情况下，IP组播路由处于关闭状态 本命令的详细介绍请参见“IP组播命令参考”中的“组播路由与转发”
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能IGMP	**igmp enable**	缺省情况下，IGMP处于关闭状态

1.3.3 配置IGMP版本

由于不同版本 IGMP 协议的报文结构与种类不同，因此需要为同一网段上的所有路由器配置相同版本的 IGMP，否则 IGMP 将不能正常运行。

表1-3 配置 IGMP 版本

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置IGMP的版本	**igmp version** *version-number*	缺省情况下，IGMP的版本为IGMPv2

1.3.4 配置静态加入

在配置了静态加入组播组或组播源组后，接口将作为该组播组的虚拟组成员存在，从而可以接收发往该组的组播数据，以测试组播数据的转发。

在配置了静态加入后，接口并不会对 IGMP 查询器发出的查询报文进行响应；当配置静态加入或取消静态加入的配置时，接口也不会主动发送 IGMP 成员关系报告报文或 IGMP 离开组报文。也就是说，该接口并没有真正成为该组播组的成员。

提示

在运行 PIM-SM 的设备上配置静态加入时，如果待配接口上同时使能了 IGMP 和 PIM-SM，则该接口必须为 PIM-SM 的 DR，否则该接口将不能加入组播组或组播源组；如果待配接口上使能了 IGMP 但未使能 PIM-SM，则该接口必须为 IGMP 查询器，否则该接口也不能加入组播组或组播源组。有关 PIM-SM 和 DR 的介绍，请参见“IP 组播配置指导”中的“PIM”。

表1-4 配置静态加入

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置静态加入组播组或组播源组	**igmp static-group** *group-address* [**source** *source-address*]	缺省情况下，接口没有以静态方式加入任何组播组或组播源组

1.3.5 配置组播组过滤器

如果不希望接口所在网段上的主机加入某些组播组，可在该接口上配置 ACL 规则作为过滤器，接口将按照该规则对收到的 IGMP 成员关系报告报文进行过滤，只为该规则所允许的组播组维护组成员关系。

表1-5 配置组播组过滤器

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置组播组过滤器	**igmp group-policy** *acl-number* [*version-number*]	缺省情况下，接口上没有配置组播组过滤器，即该接口下的主机可以加入任意组播组

说明

由于组播组过滤器只能过滤 IGMP 报文，因此无法对接口静态加入组播组或组播源组进行限制。

1.4 调整IGMP性能

1.4.1 配置准备

在调整 IGMP 性能之前，需完成以下任务：

- 配置任一单播路由协议，实现网络层互通
- 配置 IGMP 基本功能

1.4.2 配置IGMP查询

IGMPv1/v2/v3 查询器会周期性地发送 IGMP 普遍组查询报文，以判断网络上是否有组播组成员，发送间隔即为“IGMP 普遍组查询报文的发送间隔”，可以根据网络的实际情况来修改此间隔。

当同一网段上有多台组播路由器时，由 IGMP 查询器负责发送 IGMP 查询报文。如果非查询器在“其它查询器存在时间”超时前未收到来自查询器的 IGMP 查询报文，就会认为原查询器失效，从而触发新的查询器选举过程；否则，非查询器将重置“其它查询器存在时间定时器”。

提示

- 应确保 IGMP 其它查询器的存在时间大于 IGMP 普遍组查询报文的发送间隔，否则有可能导致网络内的 IGMP 查询器反复变化。
- 对 IGMP 其它查询器的存在时间所做的配置，只有当设备运行在 IGMPv2/v3 时才有效。

表1-6 配置 IGMP 查询

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置IGMP普遍组查询报文的发送间隔	**igmp query-interval** *interval*	缺省情况下，IGMP普遍组查询报文的发送间隔为125秒
配置IGMP其它查询器的存在时间	**igmp other-querier-present-interval** *interval*	缺省情况下，IGMP其它查询器的存在时间＝IGMP普遍组查询报文的发送间隔×IGMP查询器的健壮系数＋IGMP普遍组查询的最大响应时间÷2

1.4.3 配置组播组成员快速离开

提示

只有当设备运行在 IGMPv2 或 IGMPv3 时，本配置才有效。

在某些应用（如 ADSL 拨号上网）中，IGMP 查询器的一个端口唯一对应着一台接收者主机，当主机在多个组播组间频繁切换（如进行电视选台）时，为了快速响应主机的离开组报文，可以在 IGMP 查询器上开启 IGMP 快速离开功能。

在使能了 IGMP 快速离开功能之后，当 IGMP 查询器收到来自主机的离开组报文时，不再发送 IGMP 特定组查询报文或 IGMP 特定源组查询报文，而是直接向上游发送离开通告，这样一方面减小了响应延迟，另一方面也节省了网络带宽。

表1-7 配置组播组成员快速离开

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能组播组成员快速离开功能	**igmp fast-leave** [**group-policy** *acl-number*]	缺省情况下，组播组成员快速离开功能处于关闭状态

1.5 配置IGMP SSM Mapping

在 SSM 网络中，由于各种可能的限制，某些接收者主机只能运行 IGMPv1 或 IGMPv2。为了向这些仅支持 IGMPv1 或 IGMPv2 的接收者主机提供 SSM 服务，可以在路由器上配置 IGMP SSM Mapping 规则。

提示

由于 IGMP SSM Mapping 不会对 IGMPv3 的报告报文进行处理，因此为保证本网段内运行任意版本 IGMP 的接收者主机都能得到 SSM 服务，建议在该网段的接口上运行 IGMPv3。

1.5.1 配置准备

在配置 IGMP SSM Mapping 规则之前，需完成以下任务：

- 配置任一单播路由协议，实现域内网络层互通
- 配置 IGMP 基本功能

1.5.2 配置过程

表1-8 配置 IGMP SSM Mapping

操作	命令	说明
进入系统视图	**system-view**	-
进入IGMP视图	**igmp** [**vpn-instance** *vpn-instance-name*]	-
配置IGMP SSM Mapping规则	**ssm-mapping** *source-address acl-number*	缺省情况下，未配置IGMP SSM Mapping规则

1.6 配置IGMP代理

1.6.1 配置准备

在配置 IGMP 代理之前，需完成以下任务：

- 配置任一单播路由协议，实现域内网络层互通

1.6.2 使能IGMP代理功能

在设备朝向组播分发树树根方向的接口上使能了 IGMP 代理功能之后，该设备就成为了 IGMP 代理设备。

提示

- 如果在一个接口上同时使能 IGMP 代理功能和 IGMP 协议，IGMP 协议将不会生效。在已使能 IGMP 代理功能的接口上配置其它 IGMP 命令时，只有 **igmp version** 命令会生效。
- 如果在一台设备上同时使能 IGMP 代理功能和组播路由协议（如 PIM 和 MSDP），组播路由协议将不会生效。而由于 IGMPv1 查询器要由 PIM 协议选举出的 DR 来充当，因此若 IGMP 代理设备的下行接口运行的是 IGMPv1，那么该接口将无法成为 DR，从而也就无法充当 IGMP 查询器。

表1-9 使能 IGMP 代理功能

操作	命令	说明
进入系统视图	**system-view**	-
使能IP组播路由，并进入MRIB视图	**multicast routing** [**vpn-instance** *vpn-instance-name*]	缺省情况下，IP组播路由处于关闭状态 本命令的详细介绍请参见“IP组播命令参考”中的“组播路由与转发”
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能IGMP代理功能	**igmp proxy enable**	缺省情况下，IGMP代理功能处于关闭状态

1.6.3 配置非查询器转发功能

组播数据通常只被查询器转发，非查询器不具备组播转发能力，这样可避免组播数据被重复转发。但如果 IGMP 代理设备的下行接口未能当选查询器，应在该接口上使能非查询器转发功能，否则下游主机将无法收到组播数据。

提示

在共享网段内存在多台 IGMP 代理设备的情况下，如果其中一台 IGMP 代理设备的下行接口已当选为查询器，不应再在其它 IGMP 代理设备的下行接口上使能非查询器转发功能，否则该网段将收到多份重复的组播数据。

表1-10 配置非查询器转发功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能非查询器转发功能	**igmp proxy forwarding**	缺省情况下，非查询器转发功能处于关闭状态

1.6.4 配置IGMP代理的负载分担功能

当在 IGMP 代理设备的多个接口上使能了 IGMP 代理功能时：

- 如果关闭了 IGMP 代理的负载分担功能，则只有 IP 地址最大的接口会转发组播流量。
- 如果使能了 IGMP 代理的负载分担功能，则可通过这些接口对组播流量按组进行负载分担。

表1-11 配置 IGMP 代理的负载分担功能

操作	命令	说明
进入系统视图	**system-view**	-
进入IGMP视图	**igmp** [**vpn-instance** *vpn-instance-name*]	-
使能IGMP代理的负载分担功能	**proxy multipath**	缺省情况下，IGMP代理的负载分担功能处于关闭状态

1.7 IGMP显示和维护

注意

执行 **reset igmp group** 命令可能导致接收者中断组播信息的接收。

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 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 的统计信息。

表1-12 IGMP 显示和维护

操作	命令
显示IGMP组播组的信息	**display igmp** [**vpn-instance** *vpn-instance-name*] **group** [*group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**]
显示接口上IGMP配置和运行信息	**display igmp** [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**proxy**] [**verbose**]
显示IGMP代理记录的组播组信息	**display igmp** [**vpn-instance** *vpn-instance-name*] **proxy group** [*group-address* | **interface** *interface-type interface-number*] [**verbose**]
显示IGMP代理路由表的信息	**display igmp** [**vpn-instance** *vpn-instance-name*] **proxy routing-table** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }]] * [**verbose**]
显示IGMP SSM Mapping规则	**display igmp** [**vpn-instance** *vpn-instance-name*] **ssm-mapping** *group-address*
清除IGMP组的动态加入记录	**reset igmp** [**vpn-instance** *vpn-instance-name*] **group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *mask* | *mask-length* }] [*source-address* [**mask** { *mask* | *mask-length* }]] } }

说明

reset igmp group 命令只能清除动态加入记录，无法清除静态加入记录。

1.8 IGMP典型配置举例

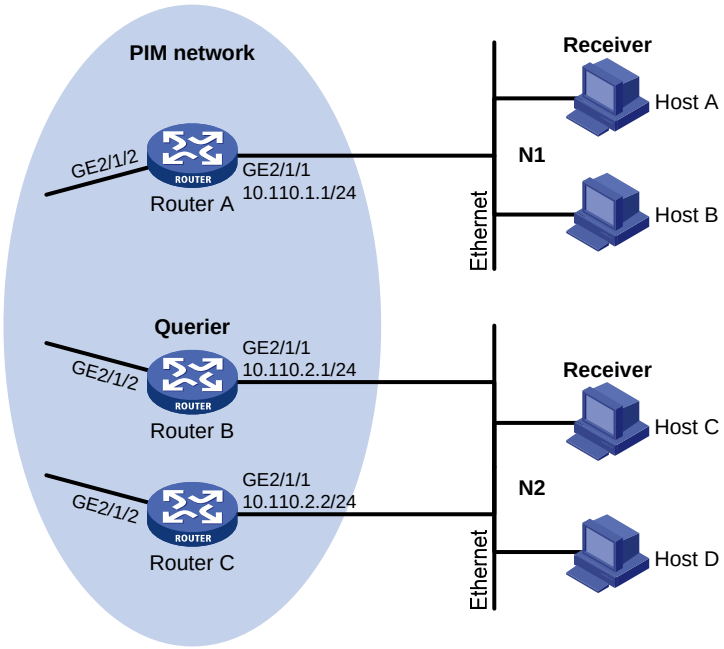
1.8.1 IGMP基本功能配置举例

1. 组网需求

- 接收者通过组播方式接收视频点播信息，不同组织的接收者组成末梢网络 N1 和 N2，Host A 与 Host C 分别为 N1 和 N2 中的组播信息接收者。
- PIM 网络中的 Router A 连接 N1，Router B 与 Router C 共同连接 N2。
- Router A 通过 GigabitEthernet2/1/1 连接 N1，通过 GigabitEthernet2/1/2 连接 PIM 网络中的其它设备。
- Router B 与 Router C 分别通过各自的 GigabitEthernet2/1/1 连接 N2，并分别通过各自的 GigabitEthernet2/1/2 连接 PIM 网络中的其它设备。
- Router A 与 N1 之间运行 IGMPv2，Router A 为 IGMP 查询器；Router B、Router C 与 N2 之间也分别运行 IGMPv2，且由于 Router B 的接口 IP 地址较小，因此由其充当 IGMP 查询器。
- 通过配置，使 N1 中的主机只能加入组播组 224.1.1.1，而对 N2 中的主机则无任何限制。

2. 组网图

图1-5 IGMP 基本功能配置组网图



3. 配置步骤

(1) 配置 IP 地址和单播路由协议

请按照 图 1-5 配置各接口的IP地址和子网掩码，具体配置过程略。

配置 PIM 网络内的各路由器之间采用 OSPF 协议进行互连，确保 PIM 网络内部在网络层互通，并且各路由器之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，并使能 PIM-DM 和 IGMP

在 Router A 上使能 IP 组播路由，在接口 GigabitEthernet2/1/2 上使能 PIM-DM，并在接口 GigabitEthernet2/1/1 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] igmp enable
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] pim dm
[RouterA-GigabitEthernet2/1/2] quit
```

在 Router B 上使能 IP 组播路由，在接口 GigabitEthernet2/1/2 上使能 PIM-DM，并在接口 GigabitEthernet2/1/1 上使能 IGMP。

```
<RouterB> system-view
[RouterB] multicast routing
[RouterB-mrib] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] igmp enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] pim dm
[RouterB-GigabitEthernet2/1/2] quit
```

在 Router C 上使能 IP 组播路由，在接口 GigabitEthernet2/1/2 上使能 PIM-DM，并在接口 GigabitEthernet2/1/1 上使能 IGMP。

```
<RouterC> system-view
[RouterC] multicast routing
[RouterC-mrib] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] igmp enable
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface gigabitethernet 2/1/2
[RouterC-GigabitEthernet2/1/2] pim dm
[RouterC-GigabitEthernet2/1/2] quit
```

(3) 配置组播组过滤器

在 Router A 上限定接口 GigabitEthernet2/1/1 下的主机只能加入组播组 224.1.1.1。

```
[RouterA] acl number 2001
[RouterA-acl-basic-2001] rule permit source 224.1.1.1 0
[RouterA-acl-basic-2001] quit
[RouterA] interface gigabitethernet 2/1/1
```

```
[RouterA-GigabitEthernet2/1/1] igmp group-policy 2001
[RouterA-GigabitEthernet2/1/1] quit
```

4. 验证配置

在 Router B 上显示接口 GigabitEthernet2/1/1 上 IGMP 配置和运行的信息。

```
[RouterB] display igmp interface gigabitethernet 2/1/1
 GigabitEthernet2/1/1(10.110.2.1):
   IGMP is enabled.
   IGMP version: 2
   Query interval for IGMP: 125s
   Other querier present time for IGMP: 255s
   Maximum query response time for IGMP: 10s
   Querier for IGMP: 10.110.2.1 (This router)
  IGMP groups reported in total: 1
```

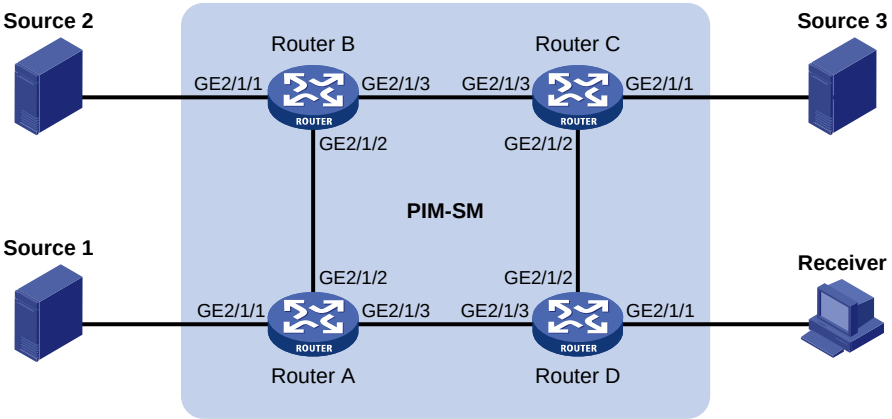
1.8.2 IGMP SSM Mapping配置举例

1. 组网需求

- PIM-SM 网络中同时采用 ASM 和 SSM 方式提供组播服务，将 Router D 的接口 GigabitEthernet2/1/3 配置为 C-BSR 和 C-RP，SSM 组播组的范围为 232.1.1.0/24。
- Router D 的接口 GigabitEthernet2/1/1 上运行 IGMPv3，接收者主机上运行 IGMPv2，且不能升级至 IGMPv3，因此该主机在加入组播组时无法指定组播源。
- Source 1、Source 2 和 Source 3 都向 SSM 组范围内的组播组发送组播数据，要求通过在 Router D 上配置 IGMP SSM Mapping 规则，使接收者主机只能接收来自 Source 1 和 Source 3 的组播数据。

2. 组网图

图1-6 IGMP SSM Mapping 配置组网图



设备	接口	IP地址	设备	接口	IP地址
Source 1	-	133.133.1.1/24	Source 3	-	133.133.3.1/24
Source 2	-	133.133.2.1/24	Receiver	-	133.133.4.1/24
Router A	GE2/1/1	133.133.1.2/24	Router C	GE2/1/1	133.133.3.2/24
	GE2/1/2	192.168.1.1/24		GE2/1/2	192.168.3.1/24
	GE2/1/3	192.168.4.2/24		GE2/1/3	192.168.2.2/24
Router B	GE2/1/1	133.133.2.2/24	Router D	GE2/1/1	133.133.4.2/24
	GE2/1/2	192.168.1.2/24		GE2/1/2	192.168.3.2/24
	GE2/1/3	192.168.2.1/24		GE2/1/3	192.168.4.1/24

3. 配置步骤

(1) 配置 IP 地址和单播路由协议

请按照 图 1-6 配置各接口的IP地址和子网掩码，具体配置过程略。

配置 PIM-SM 域内的各路由器之间采用 OSPF 协议进行互连，确保 PIM-SM 域内部在网络层互通，并且各路由器之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，并使能 PIM-SM 和 IGMP

在 Router D 上使能 IP 组播路由，在主机侧接口 GigabitEthernet2/1/1 上使能 IGMP，配置 IGMP 版本为 3；并在其它接口上使能 PIM-SM。

```
<RouterD> system-view
[RouterD] multicast routing
[RouterD-mrib] quit
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] igmp enable
[RouterD-GigabitEthernet2/1/1] igmp version 3
[RouterD-GigabitEthernet2/1/1] quit
[RouterD] interface gigabitethernet 2/1/2
[RouterD-GigabitEthernet2/1/2] pim sm
[RouterD-GigabitEthernet2/1/2] quit
[RouterD] interface gigabitethernet 2/1/3
[RouterD-GigabitEthernet2/1/3] pim sm
[RouterD-GigabitEthernet2/1/3] quit
```

在 Router A 上使能 IP 组播路由，并在各接口上使能 PIM-SM。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] pim sm
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] pim sm
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] interface gigabitethernet 2/1/3
[RouterA-GigabitEthernet2/1/3] pim sm
[RouterA-GigabitEthernet2/1/3] quit
```

Router B 和 Router C 的配置与 Router A 相似，配置过程略。

(3) 配置 C-BSR 和 C-RP

在 Router D 上配置 C-BSR 和 C-RP 的位置。

```
[RouterD] pim
[RouterD-pim] c-bsr 192.168.4.1
[RouterD-pim] c-rp 192.168.4.1
[RouterD-pim] quit
```

(4) 配置 SSM 组播组的地址范围

在 Router D 上配置 SSM 组播组的地址范围为 232.1.1.0/24。

```
[RouterD] acl number 2000
[RouterD-acl-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[RouterD-acl-basic-2000] quit
[RouterD] pim
[RouterD-pim] ssm-policy 2000
[RouterD-pim] quit
```

Router A、Router B 和 Router C 的配置与 Router D 相似，配置过程略。

(5) 配置 IGMP SSM Mapping 规则

在 Router D 上配置 IGMP SSM Mapping 规则。

```
[RouterD] igmp
[RouterD-igmp] ssm-mapping 133.133.1.1 2000
[RouterD-igmp] ssm-mapping 133.133.3.1 2000
[RouterD-igmp] quit
```

4. 验证配置

显示 Router D 上公网实例中组播组 232.1.1.1 对应的 IGMP SSM Mapping 规则。

```
[RouterD] display igmp ssm-mapping 232.1.1.1
 Group: 232.1.1.1
 Source list:
        133.133.1.1
        133.133.3.1
```

显示 Router D 上公网实例中依据 IGMP SSM Mapping 规则创建的 IGMP 组播组信息。

```
[RouterD] display igmp group
IGMP groups in total: 1
 GigabitEthernet2/1/1(133.133.4.2):
  IGMP groups reported in total: 1
   Group address   Last reporter   Uptime      Expires
   232.1.1.1       133.133.4.1     00:02:04    off
```

显示 Router D 上公网实例 PIM 路由表的内容。

```
[RouterD] display pim routing-table
 Total 0 (*, G) entry; 2 (S, G) entry

 (133.133.1.1, 232.1.1.1)
     RP: 192.168.4.1
     Protocol: pim-ssm, Flag:
     UpTime: 00:13:25
     Upstream interface: GigabitEthernet2/1/3
         Upstream neighbor: 192.168.4.2
         RPF prime neighbor: 192.168.4.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/1/1
             Protocol: igmp, UpTime: 00:13:25, Expires: -

 (133.133.3.1, 232.1.1.1)
     RP: 192.168.4.1
     Protocol: pim-ssm, Flag:
```

```
UpTime: 00:13:25
Upstream interface: GigabitEthernet2/1/2
    Upstream neighbor: 192.168.3.1
    RPF prime neighbor: 192.168.3.1
Downstream interface(s) information:
Total number of downstreams: 1
    1: GigabitEthernet2/1/1
        Protocol: igmp, UpTime: 00:13:25, Expires: -
```

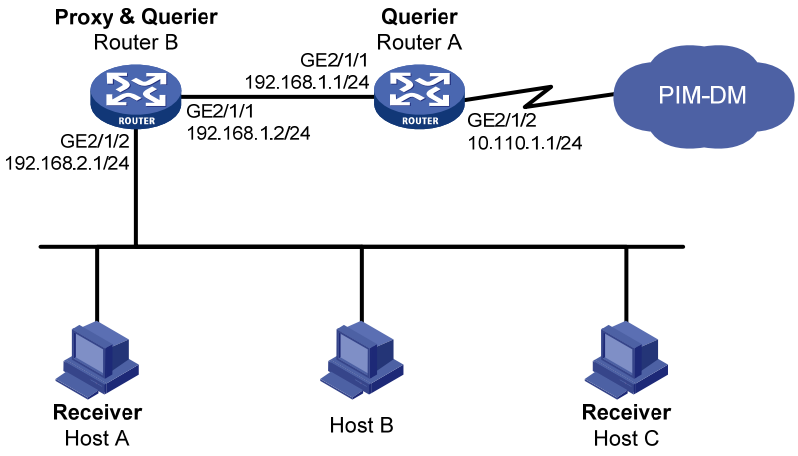
1.8.3 IGMP代理配置举例

1. 组网需求

- 核心网络中运行 PIM-DM，末梢网络中的接收者 Host A 和 Host C 通过组播组 224.1.1.1 点播视频节目。
- 要求通过在 Router B 上配置 IGMP 代理，使其在不运行 PIM-DM 的情况下实现组成员关系的维护和组播数据的正常转发。

2. 组网图

图1-7 IGMP 代理配置组网图



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) 使能 IP 组播路由，并使能 PIM-DM、IGMP 和 IGMP 代理

在 Router A 上使能 IP 组播路由，在接口 GigabitEthernet2/1/2 上使能 PIM-DM，并在接口 GigabitEthernet2/1/1 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] pim dm
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] interface gigabitethernet 2/1/1
```

```
[RouterA-GigabitEthernet2/1/1] igmp enable
[RouterA-GigabitEthernet2/1/1] quit
```

在 Router B 上使能 IP 组播路由，在接口 GigabitEthernet2/1/1 上使能 IGMP 代理，并在接口 GigabitEthernet2/1/2 上使能 IGMP。

```
<RouterB> system-view
[RouterB] multicast routing
[RouterB-mrib] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] igmp proxy enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] igmp enable
[RouterB-GigabitEthernet2/1/2] quit
```

4. 验证配置

在 Router B 上显示 IGMP 代理记录的所有组播组信息。

```
[RouterB] display igmp proxy group
IGMP proxy group records in total: 1
 GigabitEthernet2/1/1(192.168.1.2):
  IGMP proxy group records in total: 1
   Group address      Member state      Expires
   224.1.1.1          Delay             00:00:02
```

1.9 常见配置错误举例

1.9.1 接收者侧路由器上无组成员信息

1. 故障现象

当某主机发送了加入组播组 G 的报文后，离该主机最近的路由器上却没有组播组 G 的组成员信息。

2. 故障分析

- 组网、接口连线的正确与否以及接口的协议层是否 up 将直接影响组播组成员信息的生成；
- 在路由器上必须使能组播路由，在连接主机的接口上必须使能 IGMP；
- 如果路由器接口上运行的 IGMP 版本比主机的低，那么路由器将无法识别主机发来的较高版本的 IGMP 报告报文；
- 如果在接口上使用命令 **igmp group-policy** 对加入组播组 G 进行了限制后，该接口将不再接收未通过过滤的那些要求加入组播组 G 的报文。

3. 处理过程

(1) 检查组网是否正确，接口间的连线是否正确，以及接口状态是否正常，是否配置了正确的 IP 地址。通过命令 **display igmp interface** 查看接口信息。若无接口信息输出，说明接口状态异常，原因通常是接口上配置了 **shutdown** 命令，或者接口连线不正确，或者接口上没有配置正确的 IP 地址。

(2) 检查是否使能了组播路由。通过命令 **display current-configuration** 查看是否配置了命令 **multicast routing**。若缺少该配置，则需要在系统视图下执行命令 **multicast routing** 使能 IP 组播路由，同时也需要在相应接口上使能 IGMP。

(3) 检查接口上运行的 IGMP 版本。通过命令 **display igmp interface** 来检查接口上运行的 IGMP 版本是否低于主机所使用的版本。

(4) 检查接口上是否配置了 ACL 规则来限制主机加入组播组 G。通过命令 **display current-configuration interface** 观察是否配置了 **igmp group-policy** 命令。如果配置的 ACL 规则对加入组播组 G 进行了限制，则需要修改该 ACL 规则，允许接受组播组 G 的报告报文。

1.9.2 同一网段各路由器上组成员关系不一致

1. 故障现象

在同一网段的不同 IGMP 路由器上，各自维护的组成员关系不一致。

2. 故障分析

- 运行 IGMP 的路由器为每个接口维护多个参数，各参数之间相互影响，非常复杂。如果同一网段路由器的 IGMP 接口参数配置不一致，必然导致组成员关系的混乱；
- 另外，IGMP 目前有 3 个版本，版本不同的 IGMP 路由器与主机之间虽然可以部分兼容，但是连接在同一网段的所有路由器必须运行相同版本的 IGMP。如果同一网段路由器的 IGMP 版本不一致，也将导致 IGMP 组成员关系的混乱。

3. 处理过程

(1) 检查 IGMP 配置。通过命令 **display current-configuration** 观察接口上 IGMP 的配置信息。

(2) 在同一网段的所有路由器上执行命令 **display igmp interface** 来检查 IGMP 相关定时器的参数，确保配置一致。

(3) 通过命令 **display igmp interface** 来检查各路由器上运行的 IGMP 版本是否一致。

目 录

1 PIM

1.1 PIM简介

PIM（Protocol Independent Multicast，协议无关组播）协议利用单播静态路由或者任意单播路由协议（包括 RIP、OSPF、IS-IS、BGP 等）所生成的单播路由表为 IP 组播提供路由。组播路由与所采用的单播路由协议无关，只要能够通过单播路由协议产生相应的组播路由表项即可。PIM 借助 RPF（Reverse Path Forwarding，逆向路径转发）机制实现对组播报文的转发。当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，则创建相应的组播路由表项，从而进行组播报文的转发；若 RPF 检查失败，则丢弃该报文。有关 RPF 的详细介绍，请参见“IP 组播配置指导”中的“组播路由与转发”。

根据实现机制的不同，PIM 分为以下几种类型：

- PIM-DM（Protocol Independent Multicast-Dense Mode，协议无关组播—密集模式）
- PIM-SM（Protocol Independent Multicast-Sparse Mode，协议无关组播—稀疏模式）
- BIDIR-PIM（Bidirectional Protocol Independent Multicast，双向协议无关组播，简称双向 PIM）
- PIM-SSM（Protocol Independent Multicast Source-Specific Multicast，协议无关组播－指定源组播）

为了描述方便，本文中把由支持 PIM 协议的组播路由器所组成的网络简称为“PIM 域”。

1.1.1 PIM-DM简介

PIM-DM 属于密集模式的组播路由协议，使用“推（Push）模式”传送组播数据，通常适用于组播组成员相对比较密集的小型网络，其基本原理如下：

- PIM-DM 假设网络中的每个子网都存在至少一个组播组成员，因此组播数据将被扩散（Flooding）到网络中的所有节点。然后，PIM-DM 对没有组播数据转发的分支进行剪枝（Prune），只保留包含接收者的分支。这种“扩散—剪枝”现象周期性地发生，被剪枝的分支也可以周期性地恢复成转发状态。
- 当被剪枝分支的节点上出现了组播组的成员时，为了减少该节点恢复成转发状态所需的时间，PIM-DM 使用嫁接（Graft）机制主动恢复其对组播数据的转发。

一般说来，密集模式下数据包的转发路径是有源树（Source Tree），即以组播源为“根”、组播组成员为“叶子”的一棵转发树。由于有源树使用的是从组播源到接收者的最短路径，因此也称为 SPT（Shortest Path Tree，最短路径树）。

PIM-DM 的工作机制如下：

1. 邻居发现

在 PIM 域中，路由器上每个运行了 PIM 协议的接口通过定期向本网段的所有 PIM 路由器（224.0.0.13）组播 PIM Hello 报文（以下简称 Hello 报文），以发现 PIM 邻居，维护各路由器之间的 PIM 邻居关系，从而构建和维护 SPT。

2. 构建SPT

构建 SPT 的过程也就是“扩散—剪枝”的过程：

(1) 在 PIM-DM 域中，组播源 S 向组播组 G 发送组播报文时，首先对组播报文进行扩散：路由器对该报文的 RPF 检查通过后，便创建一个（S，G）表项，并将该报文向网络中的所有下游节点转发。经过扩散，PIM-DM 域内的每个路由器上都会创建（S，G）表项。

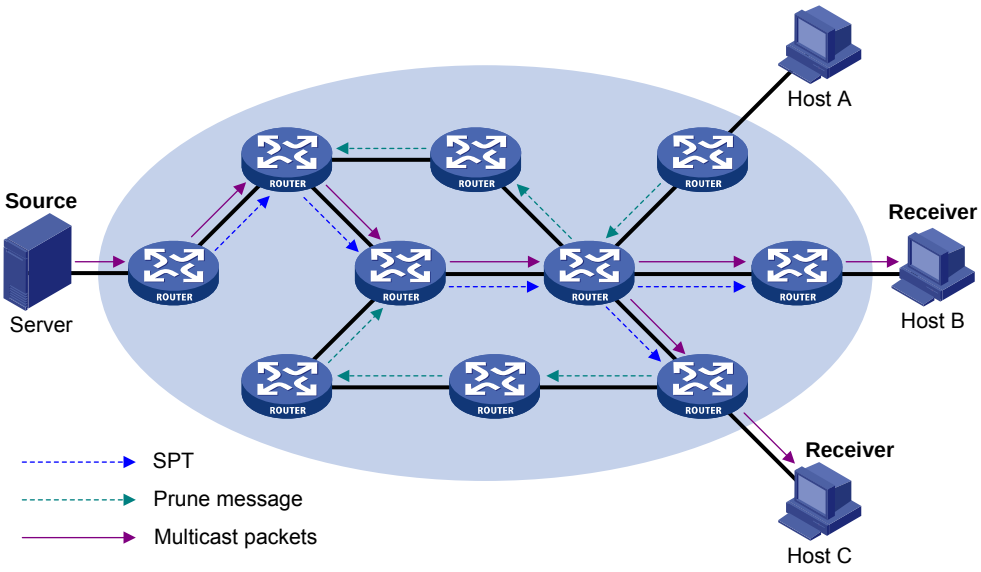
(2) 然后对那些下游没有接收者的节点进行剪枝：由没有接收者的下游节点向上游节点发剪枝报文（Prune Message），以通知上游节点将相应的接口从其组播转发表项（S，G）所对应的出接口列表中删除，并不再转发该组播组的报文至该节点。

说明

（S，G）表项包括组播源的地址 S、组播组的地址 G、出接口列表和入接口等。

剪枝过程最先由“叶子”路由器发起，如 图 1-1 所示，由没有接收者（Receiver）的接口主动发起剪枝，并一直持续到PIM-DM域中只剩下必要的分支，这些分支共同构成了SPT。

图1-1 PIM-DM 中构建 SPT 示意图



“扩散—剪枝”的过程是周期性发生的。各个被剪枝的节点提供超时机制，当剪枝超时后便重新开始这一过程。

3. 嫁接

当被剪枝的节点上出现了组播组的成员时，为了减少该节点恢复成转发状态所需的时间，PIM-DM 使用嫁接机制主动恢复其对组播数据的转发，过程如下：

(1) 需要恢复接收组播数据的节点向其上游节点发送嫁接报文（Graft Message）以申请重新加入到 SPT 中；

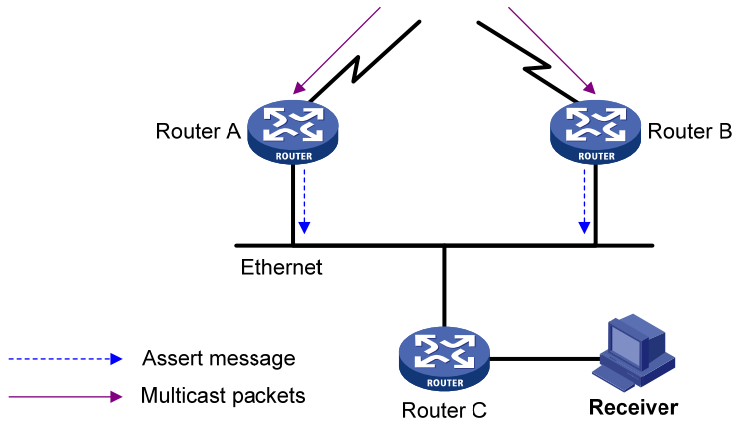
(2) 当上游节点收到该报文后恢复该下游节点的转发状态，并向其回应一个嫁接应答报文（Graft-Ack Message）以进行确认；

(3) 如果发送嫁接报文的下游节点没有收到来自其上游节点的嫁接应答报文，将重新发送嫁接报文直到被确认为止。

4. 断言

在一个网段内如果存在多台组播路由器，则相同的组播报文可能会被重复发送到该网段。为了避免出现这种情况，就需要通过断言（Assert）机制来选定唯一的组播数据转发者。

图1-2 Assert 机制示意图



如 图 1-2 所示，当Router A和Router B从上游节点收到（S，G）组播报文后，都会向本地网段转发该报文，于是处于下游的节点Router C就会收到两份相同的组播报文，Router A和Router B也会从各自的下游接口收到对方转发来的该组播报文。此时，Router A和Router B会通过其下游接口向本网段的所有PIM路由器（224.0.0.13）以组播方式发送断言报文（Assert Message），该报文中携带有以下信息：组播源地址S、组播组地址G、到组播源的单播路由/MBGP路由/组播静态路由的优先级和度量值。通过一定的规则对这些参数进行比较后，Router A和Router B中的获胜者将成为（S，G）组播报文在本网段的转发者，比较规则如下：

(1) 到组播源的优先级较高者获胜；

(2) 如果到组播源的优先级相等，那么到组播源的度量值较小者获胜；

(3) 如果到组播源的度量值也相等，则下游接口 IP 地址较大者获胜。

1.1.2 PIM-SM简介

PIM-DM 使用以“扩散—剪枝”方式构建的 SPT 来传送组播数据。尽管 SPT 的路径最短，但是其建立的过程效率较低，并不适合大中型网络。而 PIM-SM 则属于稀疏模式的组播路由协议，使用“拉（Pull）模式”传送组播数据，通常适用于组播组成员分布相对分散、范围较广的大中型网络，其基本原理如下：

- PIM-SM 假设所有主机都不需要接收组播数据，只向明确提出需要组播数据的主机转发。PIM-SM 实现组播转发的核心任务就是构造并维护 RPT（Rendezvous Point Tree，共享树），RPT 选择 PIM 域中某台路由器作为公用的根节点 RP（Rendezvous Point，汇集点），组播数据通过 RP 沿着 RPT 转发给接收者；
- 接收者侧 DR（Designated Router，指定路由器）向某组播组对应的 RP 发送加入报文（Join Message），该报文被逐跳送达 RP，所经过的路径就形成了 RPT 的分支；
- 组播源如果要向某组播组发送组播数据，首先由组播源侧 DR 负责向 RP 进行注册，把注册报文（Register Message）通过单播方式发送给 RP，该报文到达 RP 后触发建立 SPT。之后组

播源把组播数据沿着 SPT 发向 RP，当组播数据到达 RP 后，被复制并沿着 RPT 发送给接收者。

说明

复制仅发生在分发树的分支处，这个过程能够自动重复直到数据包最终到达接收者。

PIM-SM 的工作机制如下：

1. 邻居发现

PIM-SM使用与PIM-DM类似的邻居发现机制，具体请参见“1.1.1 1. 邻居发现”一节。

2. DR选举

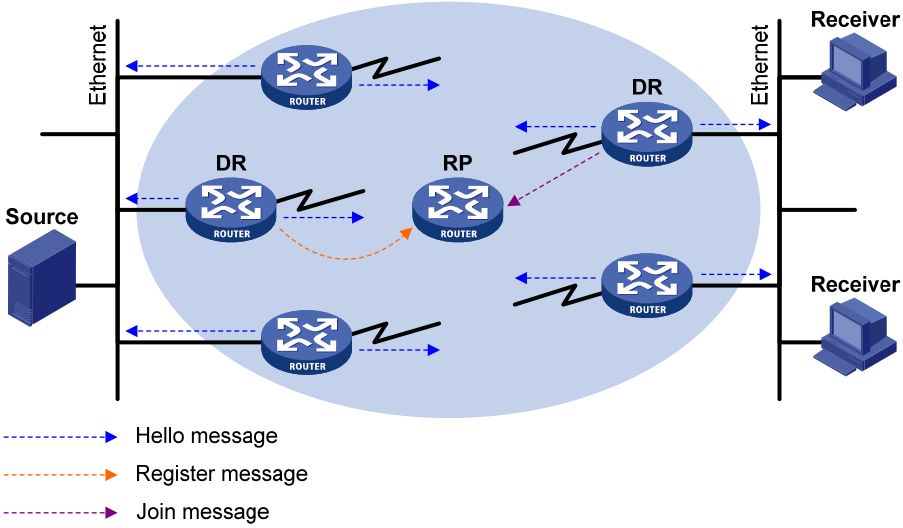
DR 是共享网络（如以太网）中组播数据的唯一转发者。无论是与组播源相连的网络，还是与接收者相连的网络，都需要选举 DR。接收者侧的 DR 负责向 RP 发送加入报文；组播源侧的 DR 负责向 RP 发送注册报文。

DR 对于 PIM-SM 有实际的意义，而对于 PIM-DM 来说，其本身并不需要 DR，但如果 PIM-DM 域中的共享网络上运行了 IGMPv1，则需要由 DR 来充当共享网络上的 IGMPv1 查询器。

提示

在充当接收者侧 DR 的设备上必须使能 IGMP，否则连接在该 DR 上的接收者将无法通过该 DR 加入组播组。有关 IGMP 的详细介绍，请参见“IP 组播配置指导”中的“IGMP”。

图1-3 DR 选举示意图



如 图 1-3 所示，DR的选举过程如下：

(1) 共享网络上的各路由器相互之间发送 Hello 报文（携带有竞选 DR 优先级的参数），拥有最高优先级的路由器将成为 DR；

(2) 如果优先级相同，或者网络中至少有一台路由器不支持在 Hello 报文中携带竞选 DR 优先级的参数，则根据各路由器的 IP 地址大小来竞选 DR，IP 地址最大的路由器将成为 DR。

如果 DR 出现故障，将导致其 PIM 邻居可达状态定时器超时，其余路由器将触发新的 DR 选举过程。

3. RP发现

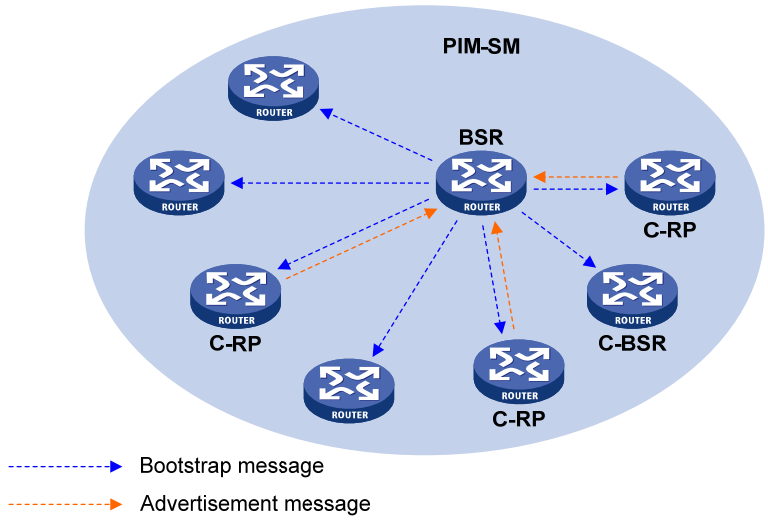
RP 是 PIM-SM 域中的核心设备。在结构简单的小型网络中，组播信息量少，整个网络仅依靠一个 RP 进行组播信息的转发即可，此时可以在 PIM-SM 域中的各路由器上静态指定 RP 的位置；但是在更多的情况下，PIM-SM 域的规模都很大，通过 RP 转发的组播信息量巨大。为了缓解 RP 的负担并优化 RPT 的拓扑结构，可以在 PIM-SM 域中配置多个 C-RP（Candidate-RP，候选 RP），通过自举机制来动态选举 RP，使不同的 RP 服务于不同的组播组，此时需要配置 BSR（Bootstrap Router，自举路由器）。BSR 是 PIM-SM 域的管理核心，一个 PIM-SM 域内只能有一个 BSR，但可以配置多个 C-BSR（Candidate-BSR，候选 BSR）。这样，一旦 BSR 发生故障，其余 C-BSR 能够通过自动选举产生新的 BSR，从而确保业务免受中断。

说明

- 一个 RP 可以同时服务于多个组播组，但一个组播组只能唯一对应一个 RP。
- 一台设备可以同时充当 C-RP 和 C-BSR。

如 图 1-4 所示，BSR负责收集网络中由C-RP发来的宣告报文（Advertisement Message），该报文中携带有C-RP的地址和优先级以及其服务的组范围，BSR将这些信息汇总为RP-Set（RP集，即组播组与RP的映射关系数据库），封装在自举报文（Bootstrap Message，BSM）中并发布到整个PIM-SM域。

图1-4 RP 与 BSR 信息交互示意图



网络中的各路由器将依据 RP-Set 提供的信息，使用相同的规则从众多 C-RP 中为特定组播组选择其对应的 RP，具体规则如下：

(1) 首先比较 C-RP 所服务的组范围，所服务的组范围较小者获胜。

(2) 若服务的组范围相同，再比较 C-RP 的优先级，优先级较高者获胜。

(3) 若优先级也相同，再使用哈希（Hash）函数计算哈希值，哈希值较大者获胜。

(4) 若哈希值也相同，则 C-RP 的 IP 地址较大者获胜。

4. Anycast-RP

PIM-SM 要求每个组播组只能有一个激活的 RP，因此当某 RP 失效时，可能导致其对应组播组的流量中断。Anycast-RP 机制通过为同一组播组设置具有相同地址的多个 RP，组播源和接收者各自就近选择 RP 进行注册或加入，这些 RP 之间则进行组播源信息的同步，从而实现了 RP 间的冗余备份。Anycast-RP 具有以下优点：

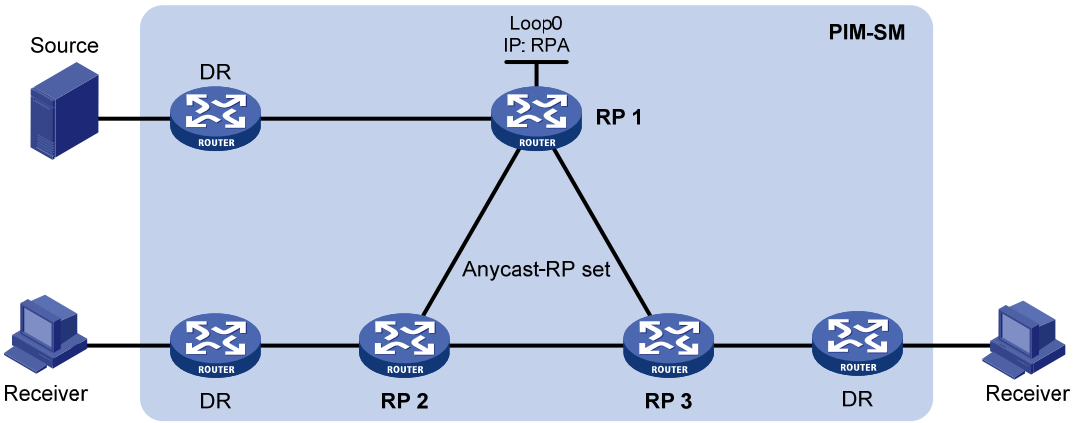
- RP 路径最优：组播源向距离最近的 RP 进行注册，建立路径最优的 SPT；接收者向距离最近的 RP 发起加入，建立路径最优的 RPT。
- RP 冗余备份：当某 RP 失效后，原先在该 RP 上注册或加入的组播源或接收者会自动选择就近的 RP 进行注册或加入，从而实现了 RP 间的冗余备份。

Anycast-RP 可以通过以下两种方式实现：

- 基于 MSDP 实现：通过为同一组播组设置具有相同地址的多个 RP，并在这些 RP 之间建立 MSDP 对等体关系来实现。详细介绍请参见“IP 组播配置指导”中的“MSDP”。
- 基于 PIM-SM 实现：通过对 RP 进行一定的扩展来实现，不需要依赖 MSDP。本文主要介绍这种实现方式。

在基于PIM-SM的实现中，由服务于同一组播组的多个RP组成的集合称为Anycast-RP集，这些RP则称为Anycast-RP成员，各成员的地址称为Anycast-RP成员地址，而Anycast-RP集对外统一发布的地址则称为Anycast-RP地址。如 图 1-5 所示，一个Anycast-RP集中包含RP 1、RP 2 和RP 3 三个成员，Anycast-RP地址为RPA。

图1-5 基于 PIM-SM 实现 Anycast-RP 示意图



基于 PIM-SM 实现 Anycast-RP 的工作过程如下：

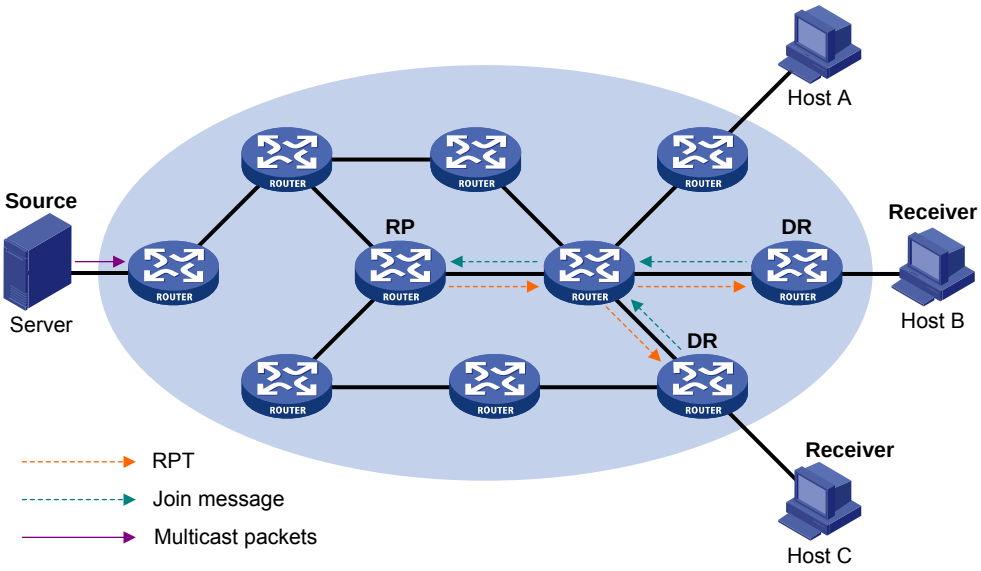
(1) RP 1 收到一个目的地址为 RPA 的注册报文，发现其源地址不是其它成员（RP 2 或 RP 3）的地址，于是认为此报文由 DR 发来。然后 RP 1 将该报文的源地址改为自己的地址后发送给所有其它成员（RP 2 和 RP 3）。如果一台设备既是 DR 也是 RP，则相当于收到自己发送的注册报文，也要向所有其它成员转发。

(2) RP 2 和 RP 3 收到 RP 1 发来的注册报文后，发现其源地址是 Anycast-RP 集的成员地址，于是不再向外转发。

由此可见，RP 接收注册报文的原有处理没有任何改变，唯一的变化就是满足条件的 RP 要向同一 Anycast-RP 集内的其它成员转发注册报文，以实现组播源信息的共享。

5. 构建RPT

图1-6 PIM-SM 中构建 RPT 示意图



如 图 1-6 所示，RPT的构建过程如下：

(1) 当接收者加入一个组播组 G 时，先通过 IGMP 报文通知与其直连的 DR；

(2) DR 掌握了组播组 G 的接收者的信息后，向该组所对应的 RP 方向逐跳发送加入报文；

(3) 从 DR 到 RP 所经过的路由器就形成了 RPT 的分支，这些路由器都在其转发表中生成了（*，G）表项，这里的“*”表示来自任意组播源。RPT 以 RP 为根，以 DR 为叶子。

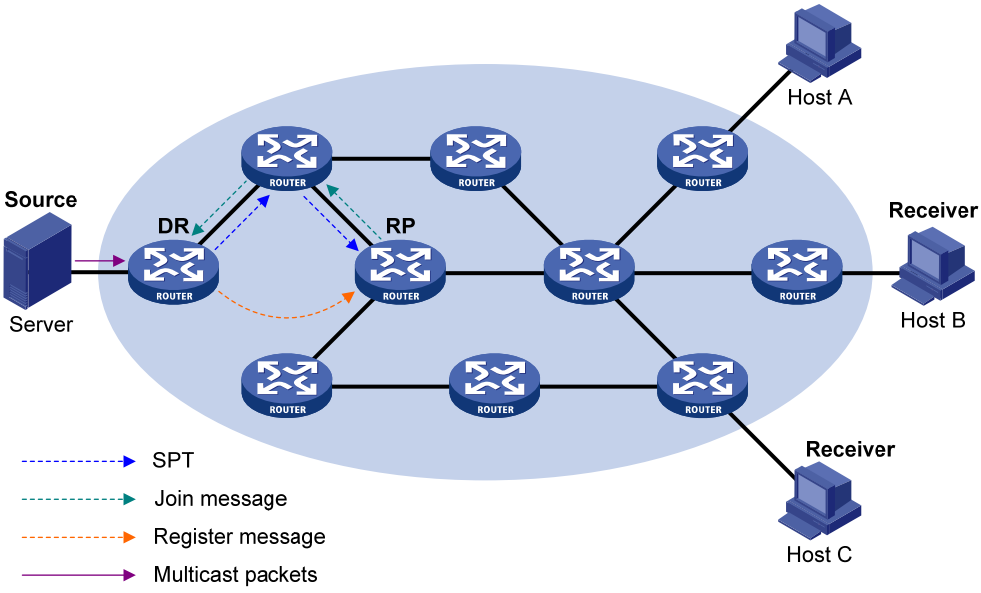
当发往组播组 G 的组播数据流经 RP 时，数据就会沿着已建立好的 RPT 到达 DR，进而到达接收者。

当某接收者对组播组 G 的信息不再感兴趣时，与其直连的 DR 会逆着 RPT 向该组的 RP 方向逐跳发送剪枝报文；上游节点收到该报文后在其出接口列表中删除与下游节点相连的接口，并检查自己是否拥有该组播组的接收者，如果没有则继续向其上游转发该剪枝报文。

6. 组播源注册

组播源注册的目的是向 RP 通知组播源的存在。

图1-7 组播源注册示意图



如 图 1-7 所示，组播源向RP注册的过程如下：

(2) 当组播源 S 向组播组 G 发送了一个组播报文时，与组播源直连的 DR 在收到该报文后，就将其封装成注册报文，并通过单播方式发送给相应的 RP；

(3) 当 RP 收到该报文后，一方面解封装注册报文并将封装在其中的组播报文沿着 RPT 转发给接收者，另一方面向组播源方向逐跳发送（S，G）加入报文。这样，从 RP 到组播源所经过的路由器就形成了 SPT 的分支，这些路由器都在其转发表中生成了（S，G）表项。

(4) 组播源发出的组播数据沿着已建立好的 SPT 到达 RP，然后由 RP 把组播数据沿着 RPT 向接收者进行转发。当 RP 收到沿着 SPT 转发来的组播数据后，通过单播方式向与组播源直连的 DR 发送注册停止报文（Register-Stop Message），组播源注册过程结束。

说明

上述描述中假定允许 RP 发起 SPT 切换，否则组播源侧 DR 将一直用注册报文封装组播报文，注册过程不会结束。

7. SPT切换

在 PIM-SM 域中，一个组播组唯一对应一个 RP 和一棵 RPT。在 SPT 切换前，所有发往该组的组播报文都必须先由组播源侧 DR 封装在注册报文中发往 RP，由 RP 解封装后再沿 RPT 分发给接收者侧的 DR，RP 是所有组播数据必经的中转站。这个过程存在以下三个问题：

- 组播源侧的 DR 和 RP 必须对组播数据进行繁琐的封装/解封装处理。
- 组播数据的转发路径不一定是从组播源到接收者的最短路径。
- 当组播流量变大时，RP 负担增大，容易引发故障。

为了解决上述问题，当组播数据的转发速率超过阈值时，PIM-SM 允许由 RP 或接收者侧的 DR 发起 SPT 切换：

(1) RP 发起的 SPT 切换

RP 周期性地检测组播数据（S，G）的转发速率，一旦发现其超过阈值，立即向组播源方向发送（S，G）加入报文，建立 RP 到组播源的 SPT 分支，后续的组播报文都直接沿该分支到达 RP。

由RP发起的SPT切换的详细过程，请参见“1.1.2 6. 组播源注册”一节。

(2) 接收者侧 DR 发起的 SPT 切换

接收者侧 DR 周期性地检测组播数据（S，G）的转发速率，一旦发现其超过阈值，立即发起 SPT 切换，过程如下：

- 首先，接收者侧 DR 向组播源方向发送（S，G）加入报文，沿途经过的所有路由器在其转发表中都生成了（S，G）表项，从而建立了 SPT 分支；
- 随后，当组播数据沿 SPT 到达 RPT 与 SPT 分叉的路由器时，该路由器开始丢弃沿 RPT 到达的组播数据，同时向 RP 逐跳发送含 RP 位的剪枝报文，RP 收到该报文后继续向组播源方向发送剪枝报文（假设此时只有这一个接收者），从而完成了 SPT 切换；
- 最终，组播数据将沿 SPT 从组播源到达到接收者。

通过 SPT 切换，PIM-SM 能够以比 PIM-DM 更经济的方式建立 SPT。

8. 断言

PIM-SM使用与PIM-DM类似的断言机制，具体请参见“1.1.1 4. 断言”一节。

1.1.3 双向PIM简介

在某些组网应用（譬如多方电视电话会议）中，同时存在多个接收者和多个组播源，在这种情况下，如果使用传统的 PIM-DM 或 PIM-SM 按 SPT 转发组播数据，需在每台路由器上针对每个组播源都创建（S，G）表项，这将占用大量的系统资源。为了解决这个问题，提出了双向 PIM 的概念。双向 PIM 由 PIM-SM 发展而来，它通过建立以 RP 为中心、分别连接组播源和接收者的双向 RPT，使组播数据沿着双向 RPT 从组播源经由 RP 转发到接收者。这样，在每台路由器上只需维护（*，G）表项即可，从而节约了系统资源。

双向 PIM 主要适用于组播源和接收者都比较密集的网络，其工作机制如下：

1. 邻居发现

双向PIM使用与PIM-SM完全相同的邻居发现机制，具体请参见“1.1.2 1. 邻居发现”一节。

2. RP发现

双向PIM使用与PIM-SM完全相同的RP发现机制，具体请参见“1.1.2 3. RP发现”一节。

PIM-SM 的 RP 必须指定为一个实际存在的 IP 地址，而双向 PIM 的 RP 则可以指定为一个实际不存在的 IP 地址，简称 RPA（Rendezvous Point Address，汇集点地址）。RPA 所属网段对应的链路就称为 RPL（Rendezvous Point Link，汇集点链路），连接到 RPL 上的所有接口都可以充当 RP，且互为备份。

说明

双向 PIM 中的 RPF 接口是指向 RP 的接口，RPF 邻居自然就是到达 RP 的下一跳地址。

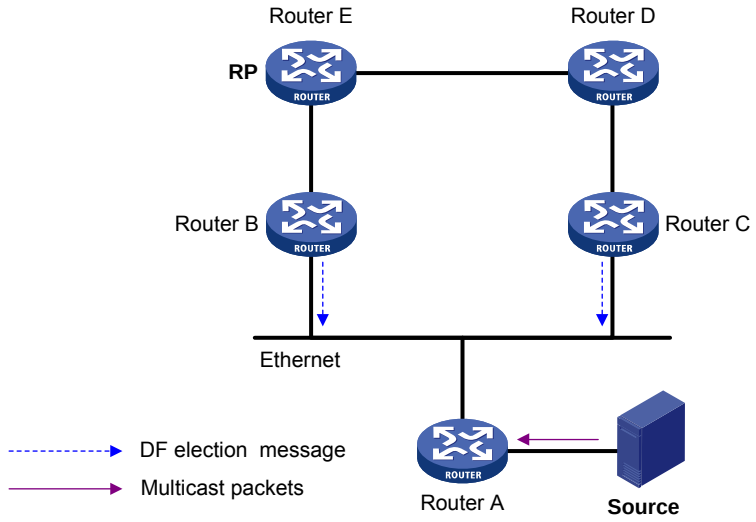
3. DF选举

DF（Designated Forwarder，指定转发者）是双向 PIM 中的重要角色，组播数据由组播源向 RP 转发的动力来自于 DF，也就是说只有 DF 才有能力将组播数据向 RP 方向转发。因此，每个 RP 在每个网段都需要有其对应的 DF，以负责将该网段的组播数据向该 RP 转发；此外，在有多台组播路由器的网段，DF 的唯一性也可以避免相同的组播报文被重复发往 RP。

说明

在 RPL 上不需要选举 DF。

图1-8 DF 选举示意图



如 图 1-8 所示，Router B和Router C都可以从Router A收到由组播源向组播组G发送的组播报文，如果它们都向下游节点转发该报文，RP最终将收到两份相同的组播报文。因此，Router B和Router C一旦获得RP的信息，就会为该RP发起DF的选举：Router B和Router C将分别向本网段的所有PIM路由器（224.0.0.13）以组播方式发送DF选举报文（DF Election Message），该报文携带有以下信息：RP的地址、到RP的单播路由/MBGP路由/组播静态路由的优先级和度量值。通过一定规则对这些参数进行比较后，Router B和Router C中的获胜者将成为DF，具体的比较规则如下：

(1) 到 RP 的优先级较高者获胜；

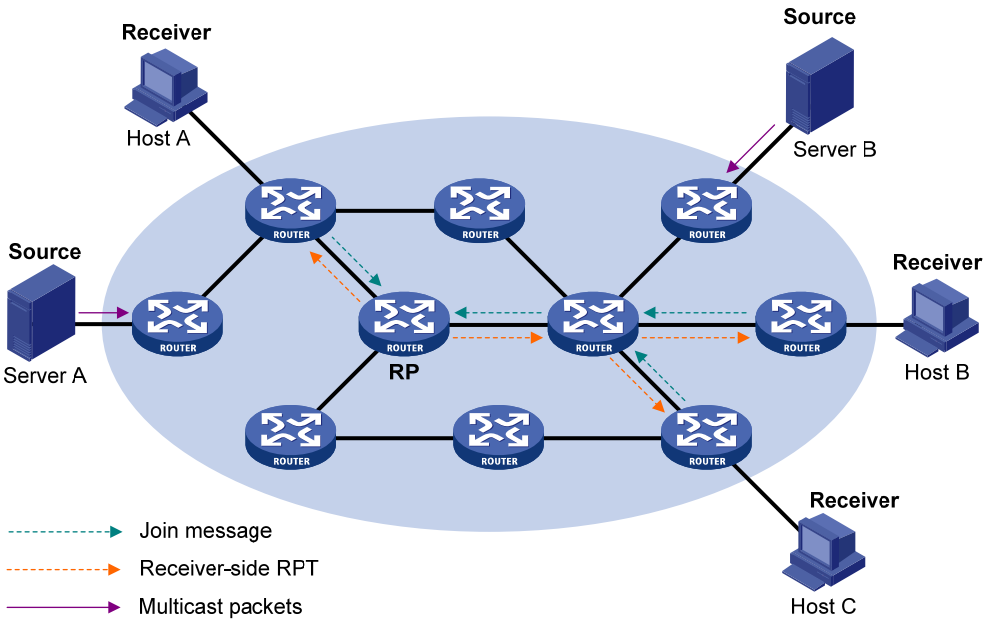
(2) 如果到 RP 的优先级相等，那么到 RP 的度量值较小者获胜；

(3) 如果到 RP 的度量值也相等，则接口的 IP 地址较大者获胜。

4. 构建双向RPT

双向 RPT 由两部分构成：一部分是以 RP 为根、以直连接收者的路由器为叶子的 RPT，简称接收者侧 RPT；而另一部分则是以 RP 为根、以直连组播源的路由器为叶子的 RPT，简称组播源侧 RPT。这两部分 RPT 的构建过程不同，下面分别加以介绍。

图1-9 接收者侧 RPT 构建示意图



接收者侧RPT的构建过程与PIM-SM中RPT的构建过程类似，如 图 1-9 所示，其构建过程如下：

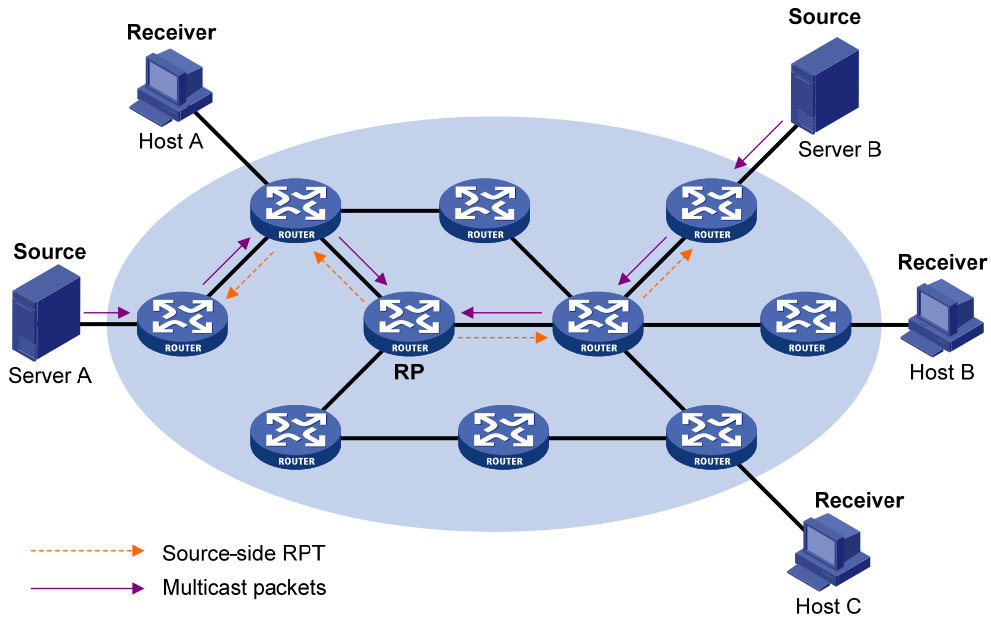
(1) 当接收者加入一个组播组 G 时，先通过 IGMP 报文通知与其直连的路由器；

(2) 该路由器掌握了组播组 G 的接收者的信息后，向该组所对应的 RP 方向逐跳发送加入报文；

(3) 从直连接收者的路由器到 RP 所经过的路由器就形成了接收者侧 RPT 的分支，这些路由器都在其转发表中生成了（*，G）表项。

当某接收者对组播组 G 的信息不再感兴趣时，与其直连的路由器会逆着接收者侧 RPT 向该组的 RP 方向逐跳发送剪枝报文；上游节点收到该报文后在其出接口列表中删除与下游节点相连的接口，并检查自己是否拥有该组播组的接收者，如果没有则继续向其上游转发该剪枝报文。

图1-10 组播源侧 RPT 构建示意图



组播源侧RPT的构建过程则相对简单，如 图 1-10 所示，其构建过程如下：

(1) 组播源发向组播组 G 的组播数据在途径的每个网段，都被该网段的 DF 无条件地向 RP 转发；

(2) 从直连组播源的路由器到 RP 所经过的路由器就形成了组播源侧 RPT 的分支，这些路由器都在其转发表中生成了（*，G）表项。

当双向 RPT 构建完成之后，由组播源发出的组播数据将依次沿着组播源侧 RPT 和接收者侧 RPT，经由 RP 转发至接收者。

说明

当接收者和组播源位于 RP 同一侧时，组播源侧 RPT 与接收者侧 RPT 有可能在到达 RP 之前就已汇合。在这种情况下，由该组播源发往该接收者的组播数据将在此汇合点直接被转发给该接收者，而不必经由 RP。

1.1.4 管理域机制简介

1. 两种域机制的划分

一般情况下，在一个 PIM-SM/双向 PIM 域内只能有一个 BSR，并由该 BSR 负责在整个 PIM-SM/双向 PIM 域内宣告 RP-Set 信息，所有组播组的信息都在此 BSR 管理的网络范围内进行转发，我们称之为非管理域机制。

考虑到管理的精细化，可以将整个 PIM-SM/双向 PIM 域划分为一个 Global 域（Global-scope Zone）和多个管理域（Admin-scope Zone），一方面可以有效分担单一 BSR 的管理压力，另一方面可以使用私有组地址为特定区域提供专门的服务。相应地，我们称之为管理域机制。

管理域与组播组相对应，针对不同组播组划分相应的管理域。管理域的边界由 ZBR（Zone Border Router，区域边界路由器）构成，每个管理域各维护一个 BSR，为特定范围的组播组服务，属于此

范围的组播协议报文（如断言报文、BSR 自举报文等）无法通过管理域边界。不同管理域所服务的组播组范围可以重叠，该范围内的组播组只在本管理域内有效，相当于私有组地址。而不属于任何管理域服务范围的组播组则一律属于 Global 域的服务范围，Global 域中维护一个 BSR，为剩余的所有组播组服务。

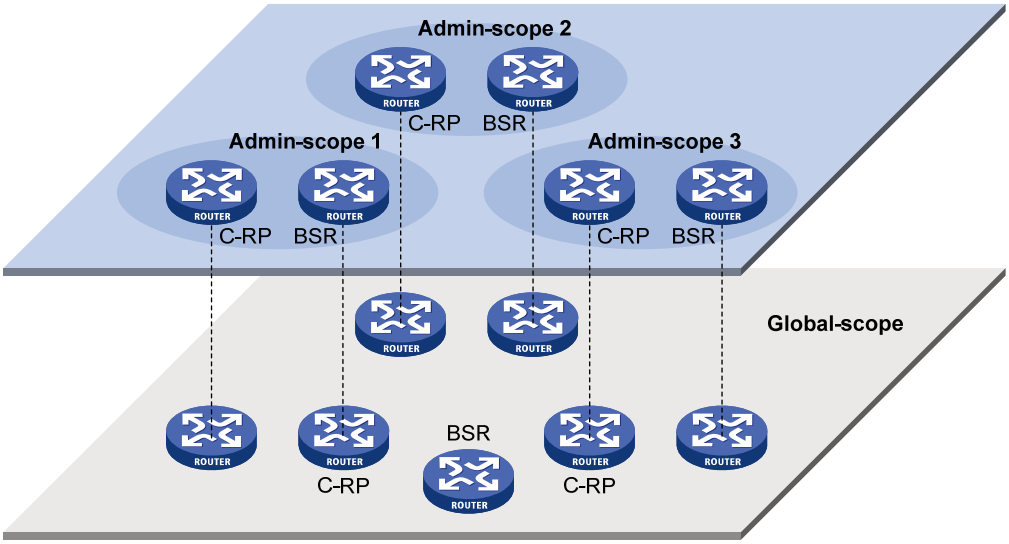
2. 管理域与Global域的关系

每个管理域以及 Global 域都有独立的 C-RP 和 BSR 设备，这些设备仅在其所属的域有效，也就是说 BSR 机制与 RP 选举在各管理域之间是隔离的；每个管理域都有自己的边界，各管理域所服务组播组范围内的组播信息不能进、出该边界。为了更清晰地理解管理域和 Global 域之间的关系，可以从以下两个角度进行考虑：

(1)　地域空间角度

管理域是针对特定范围组播组的逻辑管理区域，属于此范围的组播报文只能在本管理域的域内或域外传播，无法跨过管理域的边界。

图1-11 地域空间上管理域与 Global 域的关系

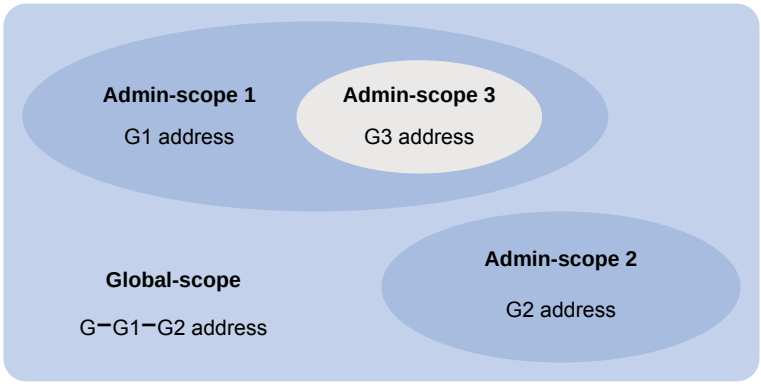


如 图 1-11 所示，对于同一地址范围内的组播组而言，各管理域在地域上必须相互独立、相互隔离，即同一路由器不能从属于多个管理域，各管理域所包含的路由器也互不相同。而Global域则包含了PIM-SM/双向PIM域内的所有路由器，不属于任何管理域服务范围的组播报文，可以在整个PIM-SM/双向PIM域范围内传播。

(2)　组地址范围角度

每个管理域为特定的组播组提供服务，这些组播组地址只在本管理域内有效，不同管理域所服务的组播组地址范围可以重叠；而不属于任何管理域的组播组，则一律属于 Global 域的服务范围。

图1-12 组地址范围上管理域与 Global 域的关系



如 图 1-12 所示，管理域 1 与管理域 2 所对应的组地址范围无交集，而管理域 3 的组地址是管理域 1 组地址的子集；其余不属于任何管理域的组播组（即G-G1-G2）则都属于Global域的服务范围。

1.1.5 PIM-SSM简介

目前，ASM（Any-Source Multicast，任意信源组播）模型包括 PIM-DM 和 PIM-SM 两种模式，SSM（Source-Specific Multicast，指定信源组播）模型能够借助 PIM-SM 的部分技术来实现，也称为 PIM-SSM。

SSM 模型为指定源组播提供了解决方案，通过 IGMPv3 来维护主机与路由器之间的关系。在实际应用中，通常采用 IGMPv3 以及 PIM-SM 的一部分技术来实现 SSM 模型。由于接收者预先已知道组播源的具体位置，因此在 SSM 模型中无需 RP，无需构建 RPT，无需组播源注册过程，也无需通过 MSDP（Multicast Source Discovery Protocol，组播源发现协议）来发现其它 PIM 域内的组播源。

PIM-SSM 的工作机制如下：

1. 邻居发现

PIM-SSM使用与PIM-SM完全相同的邻居发现机制，具体请参见“1.1.2 1. 邻居发现”一节。

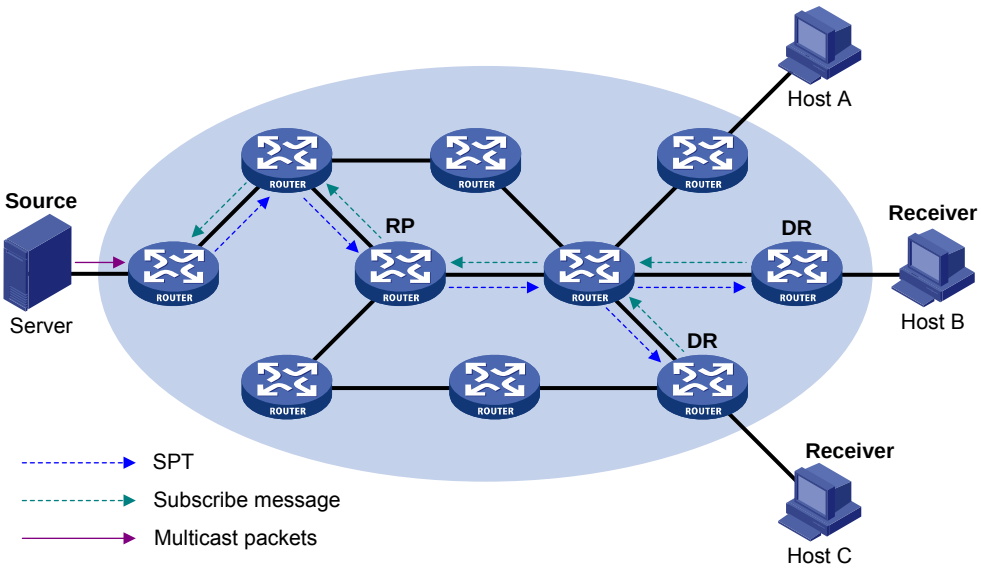
2. DR选举

PIM-SSM使用与PIM-SM完全相同的DR选举机制，具体请参见 “1.1.2 2. DR选举”一节。

3. 构建SPT

构建为 PIM-SM 服务的 RPT，还是构建为 PIM-SSM 服务的 SPT，关键在于接收者准备加入的组播组是否属于 SSM 组地址范围（IANA 保留的 SSM 组地址范围为 232.0.0.0/8）。

图1-13 PIM-SSM 中构建 SPT 示意图



如 图 1-13 所示，Host B和Host C为组播信息的接收者（Receiver），由其借助IGMPv3 的报告报文向DR报告自己对来自组播源S、发往组播组G的信息感兴趣。收到该报告报文的DR先判断该报文中的组地址是否在SSM组地址范围内：

- 如果在 SSM 组地址范围内，则构建 PIM-SSM，并向组播源 S 逐跳发送通道（Channel）的订阅报文（Subscribe Message）。沿途所有路由器上都创建（S，G）表项，从而在网络内构建了一棵以组播源 S 为根、以接收者为叶子的 SPT，该 SPT 就是 PIM-SSM 中的传输通道；
- 如果不在 SSM 组地址范围内，则仍旧按照 PIM-SM 的流程进行后续处理，此时接收者侧 DR 需要向 RP 发送（*，G）加入报文，同时组播源侧 DR 需要进行组播源的注册。

说明

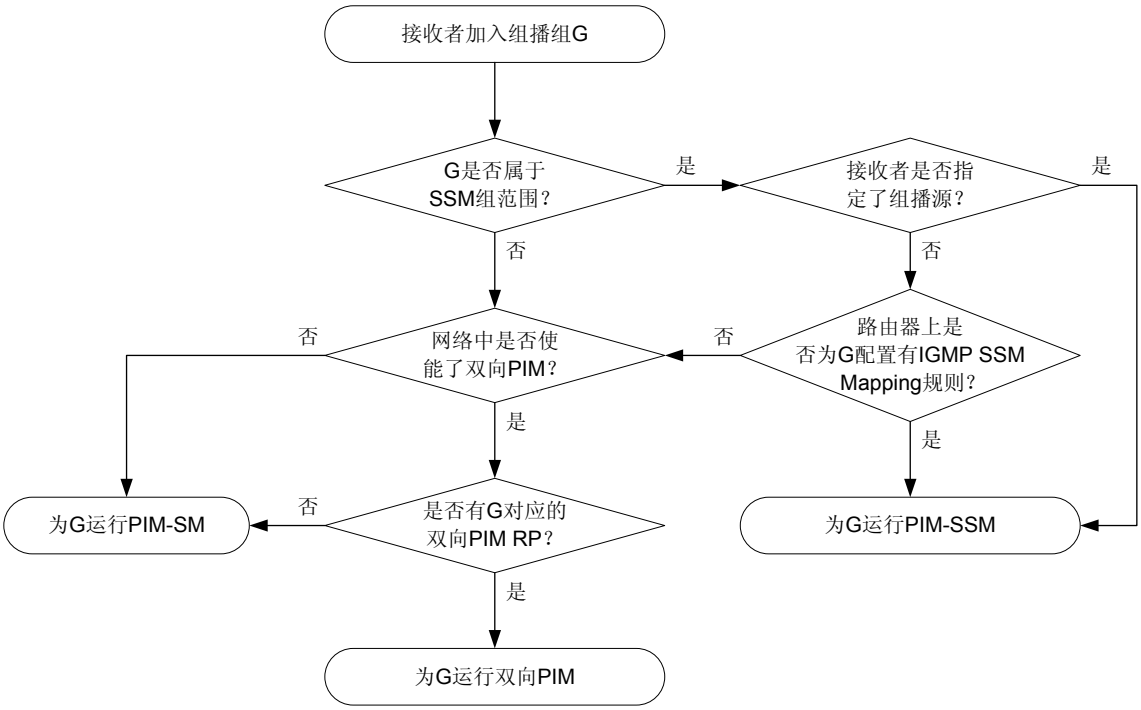
在 PIM-SSM 中，借助“通道”的概念表示组播组，借助“订阅报文”的概念表示加入报文。

1.1.6 各PIM协议运行关系

在一个 PIM 网络中，不允许 PIM-DM 与其它类型的 PIM 协议（PIM-SM、双向 PIM 和 PIM-SSM）同时运行，但允许同时运行 PIM-SM、双向 PIM 和 PIM-SSM。

当网络中同时运行PIM-SM、双向PIM和PIM-SSM时，针对具体的组加入行为运行哪种类型的PIM协议，其判断过程如 图 1-14 所示。

图1-14 各 PIM 协议运行关系示意图



有关 IGMP SSM Mapping 的详细介绍，请参见“IP 组播配置指导”中的“IGMP”。

1.1.7 多实例的PIM

在多实例应用中，组播路由器需要针对不同的实例分别维护 PIM 邻居表、组播路由表、BSR 信息和 RP-Set 信息，并保持各实例间上述信息的相互独立。

当组播路由器收到组播数据报文时，需要区分出该数据报文所属的实例，并根据该实例对应的组播路由表将其转发，或创建与该实例的 PIM 相关的组播路由表项。

1.1.8 协议规范

与 PIM 相关的协议规范有：

- RFC 3973：Protocol Independent Multicast-Dense Mode (PIM-DM): Protocol Specification (Revised)
- RFC 4601：Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised)
- RFC 4610：Anycast-RP Using Protocol Independent Multicast (PIM)
- RFC 5015：Bidirectional Protocol Independent Multicast (BIDIR-PIM)
- RFC 5059：Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
- RFC 4607：Source-Specific Multicast for IP
- draft-ietf-ssm-overview-05：An Overview of Source-Specific Multicast (SSM)

1.2 配置PIM-DM

1.2.1 PIM-DM配置任务简介

表1-1 PIM-DM 配置任务简介

配置任务	说明	详细配置
使能PIM-DM	必选	1.2.3
使能状态刷新能力	可选	1.2.4
配置状态刷新参数	可选	1.2.5
配置PIM-DM定时器	可选	1.2.6
配置PIM公共特性	可选	1.6

1.2.2 配置准备

在配置 PIM-DM 之前，需完成以下任务：

- 配置任一单播路由协议，实现域内网络层互通

1.2.3 使能PIM-DM

提示

同一台设备相同实例的所有接口上启用的 PIM 模式必须相同。

在进行各项 PIM 配置之前，必须先使能 IP 组播路由。

在接口上使能了 PIM-DM 后，路由器之间才能够建立 PIM 邻居，从而对来自 PIM 邻居的协议报文进行处理。在部署 PIM-DM 域时，建议在其所有非边界接口上均使能 PIM-DM。

表1-2 使能 PIM-DM

操作	命令	说明
进入系统视图	**system-view**	-
使能IP组播路由，并进入MRIB视图	**multicast routing** [**vpn-instance** *vpn-instance-name*]	缺省情况下，IP组播路由处于关闭状态 本命令的详细介绍请参见“IP组播命令参考”中的“组播路由与转发”
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能PIM-DM	**pim dm**	缺省情况下，PIM-DM处于关闭状态

1.2.4 使能状态刷新能力

为了避免各路由器上被剪枝的接口因为超时而恢复转发，与组播源直连的路由器会周期性地发送（S，G）状态刷新报文，该报文沿着 PIM-DM 域最初的扩散路径逐跳进行转发，从而刷新沿途所有路由器上的剪枝定时器的状态。只有当一个共享网段内的所有 PIM 路由器上都使能了状态刷新能力时，该共享网段才具备状态刷新能力。

请在 PIM-DM 域内的所有路由器上进行如下配置。

表1-3 使能状态刷新能力

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能状态刷新能力	**pim state-refresh-capable**	缺省情况下，状态刷新能力处于使能状态

1.2.5 配置状态刷新参数

直连组播源的路由器会以一定的时间间隔周期性地发送状态刷新报文，可以在与组播源直连的路由器上通过配置来改变这个时间间隔。

路由器可能在短时间内收到多个状态刷新报文，而其中有些报文可能是重复的。为了避免接收这些重复的报文，可以配置接收新状态刷新报文的等待时间：路由器将丢弃在该时间内收到的状态刷新报文；当该时间超时后，路由器将正常接收新的状态刷新报文，并更新自己的 PIM-DM 状态，同时重置该等待时间。

在收到状态刷新报文时，路由器会将该报文的 TTL 值减 1 后转发给其下游，直至该报文的 TTL 值减为 0，当网络规模很小时，状态刷新报文将在网络中循环传递。因此，为了有效控制刷新报文的传递范围，需要根据网络规模大小在与组播源直连的路由器上配置合适的 TTL 值。

表1-4 配置状态刷新参数

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
配置发送状态刷新报文的时间间隔	**state-refresh-interval** *interval*	缺省情况下，发送状态刷新报文的时间间隔为60秒
配置接收新状态刷新报文的等待时间	**state-refresh-rate-limit** *time*	缺省情况下，接收新状态刷新报文的等待时间为30秒
配置状态刷新报文的TTL值	**state-refresh-ttl** *ttl-value*	缺省情况下，状态刷新报文的TTL值为255

1.2.6 配置PIM-DM定时器

嫁接报文是 PIM-DM 中唯一使用确认机制的报文。在 PIM-DM 域中，下游路由器发出嫁接报文后，如果在指定时间内没有收到来自其上游路由器的嫁接应答报文，则会重发嫁接报文，直到被确认。有关PIM-DM其它定时器的相关配置，请参见“1.6.6 配置PIM公共定时器”。

表1-5 配置 PIM-DM 定时器

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置嫁接报文的重传时间	**pim timer graft-retry** *interval*	缺省情况下，嫁接报文的重传时间为3秒

1.3 配置PIM-SM

1.3.1 PIM-SM配置任务简介

表1-6 PIM-SM 配置任务简介

配置任务		说明	详细配置
使能PIM-SM		必选	1.3.3
配置RP	配置静态RP	二者至少选其一，若只配置静态RP，则不必再配置BSR	1.3.4 1.
	配置C-RP		1.3.4 2.
	配置Anycast-RP	可选	1.3.4 3.
配置BSR	配置C-BSR	必选	1.3.5 1.
	配置BSR服务边界	可选	1.3.5 2.
	关闭自举报文语义分片功能	可选	1.3.5 3.
配置组播源注册		可选	1.3.6
配置SPT切换		可选	1.3.7
配置PIM公共特性		可选	1.6

1.3.2 配置准备

在配置 PIM-SM 之前，需完成以下任务：

- 配置任一单播路由协议，实现域内网络层互通

1.3.3 使能PIM-SM

提示

同一台设备相同实例的所有接口上启用的 PIM 模式必须相同。

在进行各项 PIM 配置之前，必须先使能 IP 组播路由。

在接口上使能了 PIM-SM 后，路由器之间才能够建立 PIM 邻居，从而对来自 PIM 邻居的协议报文进行处理。在部署 PIM-SM 域时，建议在其所有非边界接口上均使能 PIM-SM。

表1-7 使能 PIM-SM

操作	命令	说明
进入系统视图	**system-view**	-
使能IP组播路由，并进入MRIB视图	**multicast routing** [**vpn-instance** *vpn-instance-name*]	缺省情况下，IP组播路由处于关闭状态 本命令的详细介绍请参见“IP组播命令参考”中的“组播路由与转发”
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能PIM-SM	**pim sm**	缺省情况下，PIM-SM处于关闭状态

1.3.4 配置RP

一个 RP 可以为多个组播组服务，也可以为所有组播组服务。每个组播组在任意时刻，只能由唯一的一个 RP 为其转发数据，而不能由多个 RP 转发数据。

RP 可以通过手工方式静态配置，也可以通过 BSR 机制动态选举。由于在大型 PIM 网络中配置静态 RP 将非常繁琐，因此，通常将静态 RP 作为动态选举 RP 机制的备份手段，以提高网络的健壮性，增强组播网络的运营管理能力。

1. 配置静态RP

当网络内仅有一个动态 RP 时，可以手工配置静态 RP，既可避免因单一节点故障而引起的通信中断，也可避免 C-RP 与 BSR 之间频繁的信息交互而占用带宽。PIM-SM 域内的所有路由器上都必须进行完全相同的静态 RP 配置。

表1-8 配置静态 RP

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
配置服务于PIM-SM的静态RP	**static-rp** *rp-address* [*acl-number* | **preferred**] *	缺省情况下，没有配置静态RP

2. 配置C-RP

提示

在配置 C-RP 时，应在 C-RP 与 PIM-SM 域中的其它设备之间保留较大的通信带宽。

在 PIM-SM 域中，可以把有意成为 RP 的路由器配置为 C-RP。BSR 通过接收来自 C-RP 的 C-RP 信息，或者接收来自其它路由器的自动 RP 宣告，收集 C-RP 信息并将其汇总为 RP-Set 信息，然后在全网内扩散。之后，网络内的其它路由器根据 RP-Set 信息计算出特定组播组范围所对应的 RP。建议在骨干网路由器上配置 C-RP。

为了使 BSR 能够在 PIM-SM 域内分发 RP-Set 信息，C-RP 必须周期性地向 BSR 发送宣告报文，BSR 从该报文中学习 RP-Set 信息，并将该信息与自己的 IP 地址一起封装在自举报文中向域中的所有 PIM 路由器进行宣告。

C-RP 在其宣告报文中封装一个保持时间，BSR 在收到该报文后，从中获得该时间值并启动 C-RP 超时定时器，如果超时后 BSR 仍没有收到来自 C-RP 后续的宣告报文，则认为目前网络中的 C-RP 失效或不可达。

为了防止 C-RP 欺骗，需要在 BSR 上配置合法的 C-RP 地址范围及其服务的组播组范围。同时由于每个 C-BSR 都可能成为 BSR，因此必须在 PIM-SM 域内的所有 C-BSR 上都配置相同的过滤策略。

表1-9 配置 C-RP

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
配置C-RP	**c-rp** *ip-address* [**advertisement-interval** *adv-interval* | **group-policy** *acl-number* | **holdtime** *hold-time* | **priority** *priority*] *	缺省情况下，没有配置C-RP
（可选）配置合法的C-RP地址范围及其服务的组播组范围	**crp-policy** *acl-number*	缺省情况下，C-RP地址范围及其服务的组播组范围不受任何限制

3. 配置Anycast-RP

在配置 Anycast-RP 前，需要先在 PIM-SM 域中完成静态 RP 或 C-RP 的配置，然后将静态 RP 或动态选举出的 RP 当作 Anycast-RP 地址进行 Anycast-RP 的配置。

在配置 Anycast-RP 时，请遵循以下原则：

- Anycast-RP 集中必须包括 Anycast-RP 地址所在的设备。
- 在 Anycast-RP 集的每台成员设备上通过重复执行 **anycast-rp** 命令，将包括自己在内的所有成员的地址都添加到 Anycast-RP 集中。

提示

- Anycast-RP 地址不能再用作 BSR 的地址，否则其发出的自举报文将被其它成员设备丢弃。
- 一个 Anycast-RP 集中的成员设备不建议超过 16 台，否则将影响网络性能。
- 建议使用 LoopBack 接口的地址作为 Anycast-RP 成员地址。如果一台成员设备有多个接口的地址被添加到 Anycast-RP 集中，则采用 IP 地址最小的那个作为其成员地址，其余作为备份。

表1-10 配置 Anycast-RP

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
配置Anycast-RP	**anycast-rp** *anycast-rp-address member-rp-address*	缺省情况下，没有配置Anycast-RP

1.3.5 配置BSR

如果配置了静态 RP，则不需要配置 BSR；但如果配置了 C-RP 来动态选举 RP，则必须配置 BSR。在一个 PIM-SM 域中只能有一个 BSR，但需要配置至少一个 C-BSR。任意一台路由器都可以被配置为 C-BSR。在 C-BSR 之间通过自动选举产生 BSR，BSR 负责在 PIM-SM 域中收集并发布 RP 信息。

1. 配置C-BSR

提示

- 由于 BSR 与 PIM-SM 域中的其它设备需要交换大量信息，因此应在 C-BSR 与 PIM-SM 域中的其它设备之间保留较大的通信带宽。
- 当 C-BSR 与其它 PIM 路由器通过隧道连接时，如果单播路由中到 C-BSR 下一跳的不是 Tunnel 接口，请在 PIM 路由器上通过配置组播静态路由以保证这一点，否则将影响 RPF 检查。有关组播静态路由的相关配置，请参见“IP 组播配置指导”中的“组播路由与转发”。

C-BSR 应配置在骨干网的路由器上，C-BSR 间的自动选举机制简单描述如下：

- 最初，每个 C-BSR 都认为自己是本 PIM-SM 域的 BSR，向其它路由器发送自举报文；
- 当某 C-BSR 收到其它 C-BSR 发来的自举报文时，首先比较自己与后者的优先级，优先级较高者获胜；在优先级相同的情况下，再比较自己与后者的 BSR 地址，拥有较大 IP 地址者获胜。如果后者获胜，则用后者的 BSR 地址替换自己的 BSR 地址，并不再认为自己是 BSR；否则，保留自己的 BSR 地址，并继续认为自己是 BSR。

在一个 PIM-SM 域中，从众多 C-BSR 中选举出唯一的 BSR。PIM-SM 域内的 C-RP 向 BSR 发送宣告报文，由 BSR 汇总为 RP-Set，并向本 PIM-SM 域内的所有路由器进行宣告。所有路由器都使用统一的哈希算法，得到特定组播组所对应 RP 的地址。

通过在路由器上配置合法 BSR 的地址范围，可以对收到的自举报文按照地址范围进行过滤，从而防止某些恶意主机非法伪装成 BSR，以避免合法的 BSR 被恶意取代。必须在 PIM-SM 域内的所有路由器上进行相同的配置。通常针对以下两类情况实施预防措施：

- 某些恶意主机通过伪造自举报文以欺骗路由器，试图更改 RP 映射关系。这种攻击通常发生在边缘路由器上，由于 BSR 处于网络内部，主机在网络外部，因此边缘路由器通过对收到的自举报文进行邻居检查和 RPF 检查，丢弃不符合要求的报文，就可以避免外部网络用户对内部网络 BSR 的攻击；
- 网络中某台路由器被攻击者控制，或者有非法接入的路由器时，攻击者可以将这样的路由器配置为 C-BSR，并使其在竞争中获胜，从而控制网络中 RP 信息的发布权。由于在被配置为 C-BSR 后，路由器会自动向整个网络扩散自举报文，而自举报文是 TTL 值为 1 的组播报文，所以只要其邻居路由器不接收该自举报文，就不会影响整个网络。因此，通过在整个网络的所有路由器上都配置合法 BSR 的地址范围，从而丢弃合法范围之外的自举报文，就可以防止此类攻击。

以上两种预防措施可以部分地保护网络中 BSR 的安全。但是如果某台合法的 BSR 路由器被攻击者控制，还是可能导致问题。

表1-11 配置 C-BSR

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
配置C-BSR	**c-bsr** *ip-address* [**scope** *group-address* { *mask-length* | *mask* }] [**hash-length** *hash-length* | **priority** *priority*] *	缺省情况下，没有配置C-BSR
（可选）配置合法的BSR地址范围	**bsr-policy** *acl-number*	缺省情况下，BSR的地址范围不受任何限制

2. 配置BSR服务边界

BSR 作为 PIM-SM 域中的管理核心，负责将收集到的 RP-Set 信息以自举报文的形式发向 PIM-SM 域中的所有路由器。

BSR 的服务边界，即 PIM-SM 域的边界。BSR 是针对特定的服务范围而言的，众多的 BSR 服务边界接口将网络划分成不同的 PIM-SM 域，自举报文无法通过 PIM-SM 域的边界，BSR 服务边界之外的路由器也不能参与本 PIM-SM 域内的组播转发。

请在欲配置为 BSR 服务边界的路由器上进行如下配置。

表1-12 配置 BSR 服务边界

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置BSR的服务边界	**pim bsr-boundary**	缺省情况下，没有配置BSR的服务边界

3. 关闭自举报文语义分片功能

BSR 周期性地向所在 PIM-SM 域发送自举报文以通告 RP-Set 信息。当 RP-Set 信息较少时，自举报文被封装在一个 IP 报文中发送出去；而当 RP-Set 信息较多时，自举报文的大小可能超过接口的 MTU（Maximum Transmission Unit，最大传输单元）值，从而触发其在 IP 层的分片。在这种情况下，一个 IP 分片的丢失就会导致整个自举报文都被丢弃。

自举报文语义分片功能可以解决上述问题：当自举报文大于接口 MTU 时，会被分解为多个自举报文分片（Bootstrap Message Fragment，BSMF）。非 BSR 收到自举报文分片后，若发现某组范围对应的 RP 信息都在这一个分片中，便立即更新该组范围对应的 RP-Set；若发现某组范围映射的 RP 信息被分在了多个分片中，则待收齐了这些分片后再更新该组范围对应的 RP-Set。这样，由于不同分片所含组范围对应的 RP 信息不同，因此个别分片的丢失只影响该分片所含组范围对应的 RP 信息，而不会导致整个自举报文都被丢弃。

自举报文语义分片功能是缺省使能的，但由于不支持该功能的设备会将自举报文分片当作完整的自举报文处理，从而导致其学到的 RP-Set 信息不完整，因此当 PIM-SM 域中存在此类设备时，请在已配置为 C-BSR 的路由器上关闭本功能。

表1-13 关闭自举报文语义分片功能

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
关闭自举报文语义分片功能	**undo bsm-fragment enable**	缺省情况下，自举报文语义分片功能处于使能状态

说明

通常，BSR 根据其 BSR 接口的 MTU 值对自举报文进行语义分片；而对由于新学到 PIM 邻居而触发的自举报文发送，则根据发送接口的 MTU 值进行语义分片。

1.3.6 配置组播源注册

在 PIM-SM 域内，组播源侧 DR 向 RP 发送注册报文，而这些注册报文拥有不同的组播源或组播组地址。为了让 RP 服务于特定的组播组，可以对注册报文进行过滤。如果某个（S，G）表项被过滤规则拒绝，或者过滤规则中没有定义对它的操作，RP 都会向 DR 发送注册停止报文，以停止该组播数据的注册过程。

考虑到注册报文在传递过程中的完整性，可以配置根据整个报文来计算校验和。但为了减少往注册报文中封装数据报文的工作量并考虑到互通性，一般情况下不建议配置根据注册报文的全部内容来计算校验和的方式。

当接收者不再通过 RP 接收发往某组播组的数据（即 RP 不再服务于该组播组），或 RP 开始接收组播源沿着 SPT 发来的组播数据时，RP 将向组播源侧 DR 发送注册停止报文，DR 收到该报文后将停止发送封装有组播数据的注册报文并启动注册停止定时器（Register-Stop Timer）。在注册停止定时器超时之前，DR 会向 RP 发送一个空注册报文（Null-Register Message，即不封装组播数据的

注册报文）：如果 DR 在注册探测时间（Register_Probe_Time）内收到了来自 RP 的注册停止报文，DR 将刷新其注册停止定时器；否则，DR 将重新开始发送封装有组播数据的注册报文。

注册停止定时器的超时时间是一个随机值，由其它两个时间值决定：注册抑制时间（Register_Suppression_Time）和注册探测时间（固定为 5 秒）。其具体取值范围如下：（0.5×注册抑制时间，1.5×注册抑制时间）－注册探测时间。

请在所有已配置为 C-RP 的路由器上配置注册报文的过滤规则和根据注册报文的全部内容来计算校验和；请在所有可能成为组播源侧 DR 的路由器上配置注册抑制时间。

表1-14 配置组播源注册

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
配置注册报文的过滤规则	**register-policy** *acl-number*	缺省情况下，没有配置注册报文的过滤规则
配置根据注册报文的全部内容来计算校验和	**register-whole-checksum**	缺省情况下，仅根据注册报文头来计算校验和
配置注册抑制时间	**register-suppression-timeout** *interval*	缺省情况下，注册抑制时间为60秒

1.3.7 配置SPT切换

接收者侧 DR 和 RP 都能够周期性地检测流经本设备的组播数据的转发速率（交换机无此功能），从而触发从 RPT 切换到 SPT。

提示

- 如果组播源是通过 MSDP 学习到的，则不论阈值 *traffic-rate* 为多大，设备收到第一个组播数据包后便立即向 SPT 切换。
- 由于某些设备无法将组播报文封装在注册报文中发给 RP，因此在可能成为 RP 的设备上不建议配置永不发起 SPT 切换，以免导致组播报文转发失败。

表1-15 配置 SPT 切换

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
配置发起SPT切换的条件	**spt-switch-threshold** { *traffic-rate* | **immediacy** | **infinity** } [**group-policy** *acl-number*]	缺省情况下，设备收到第一个组播数据包后便立即向SPT切换 交换机不支持*traffic-rate*参数

1.4 配置双向PIM

1.4.1 双向PIM配置任务简介

表1-16 双向 PIM 配置任务简介

配置任务		说明	详细配置
使能双向PIM		必选	1.4.3
配置RP	配置静态RP	二者至少选其一，若只配置静态RP，则不必再配置BSR	1.4.4 1.
	配置C-RP		1.4.4 2.
	配置双向PIM RP的最大数目	可选	1.4.4 3.
配置BSR	配置C-BSR	必选	1.4.5 1.
	配置BSR服务边界	可选	1.4.5 2.
	关闭自举报文语义分片功能	可选	1.4.5 3.
配置PIM公共特性		可选	1.6

1.4.2 配置准备

在配置双向 PIM 之前，需完成以下任务：

- 配置任一单播路由协议，实现域内网络层互通

1.4.3 使能双向PIM

提示

同一台设备相同实例的所有接口上启用的 PIM 模式必须相同。

由于双向 PIM 是在 PIM-SM 的基础上实现的，因此在使能双向 PIM 之前须先使能 PIM-SM。在部署双向 PIM 域时，建议在其所有非边界接口上均使能 PIM-SM。

表1-17 使能双向 PIM

操作	命令	说明
进入系统视图	**system-view**	-
使能IP组播路由，并进入MRIB视图	**multicast routing** [**vpn-instance** *vpn-instance-name*]	缺省情况下，IP组播路由处于关闭状态 本命令的详细介绍请参见“IP组播命令参考”中的“组播路由与转发”
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能PIM-SM	**pim sm**	缺省情况下，PIM-SM处于关闭状态

操作	命令	说明
退回系统视图	**quit**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
使能双向PIM	**bidir-pim enable**	缺省情况下，双向PIM处于关闭状态

1.4.4 配置RP

提示

当 PIM 网络中同时运行 PIM-SM 和双向 PIM 时，请勿使一个 RP 同时为 PIM-SM 和双向 PIM 工作，否则可能引起 PIM 路由表出错。

一个 RP 可以为多个组播组服务，也可以为所有组播组服务。每个组播组在任意时刻，只能由唯一的一个 RP 为其转发数据，而不能由多个 RP 转发数据。

RP 可以通过手工方式静态配置，也可以通过 BSR 机制动态选举。由于在大型 PIM 网络中配置静态 RP 将非常繁琐，因此，通常将静态 RP 作为动态选举 RP 机制的备份手段，以提高网络的健壮性，增强组播网络的运营管理能力。

1. 配置静态RP

当网络内仅有一个动态 RP 时，可以手工配置静态 RP，既可避免因单一节点故障而引起的通信中断，也可避免 C-RP 与 BSR 之间频繁的信息交互而占用带宽。双向 PIM 域内的所有路由器上都必须进行完全相同的静态 RP 配置。

说明

双向 PIM 允许将静态 RP 的 IP 地址指定为一个实际不存在的 IP 地址。譬如，一条链路两端接口的 IP 地址分别为 10.1.1.1/24 和 10.1.1.2/24，可以将静态 RP 的 IP 地址指定为同网段但实际不存在的一个地址，如 10.1.1.100/24，该链路就成为了 RPL。

表1-18 配置静态 RP

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
配置服务于双向PIM的静态RP	**static-rp** *rp-address* **bidir** [*acl-number* | **preferred**] *	缺省情况下，没有配置静态RP

2. 配置C-RP

提示

在配置 C-RP 时，应在 C-RP 与双向 PIM 域中的其它设备之间保留较大的通信带宽。

在双向 PIM 域中，可以把有意成为 RP 的路由器配置为 C-RP。BSR 通过接收来自 C-RP 的 C-RP 信息，或者接收来自其它路由器的自动 RP 宣告，收集 C-RP 信息并将其汇总为 RP-Set 信息，然后在全网内扩散。之后，网络内的其它路由器根据 RP-Set 信息计算出特定组播组范围所对应的 RP。建议在骨干网路由器上配置 C-RP。

为了使 BSR 能够在双向 PIM 域内分发 RP-Set 信息，C-RP 必须周期性地向 BSR 发送宣告报文，BSR 从该报文中学习 RP-Set 信息，并将该信息与自己的 IP 地址一起封装在自举报文中向域中的所有 PIM 路由器进行宣告。

C-RP 在其宣告报文中封装一个保持时间，BSR 在收到该报文后，从中获得该时间值并启动 C-RP 超时定时器，如果超时后 BSR 仍没有收到来自 C-RP 后续的宣告报文，则认为目前网络中的 C-RP 失效或不可达。

表1-19 配置 C-RP

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
配置服务于双向PIM的C-RP	**c-rp** *ip-address* [**advertisement-interval** *adv-interval* | **group-policy** *acl-number* | **holdtime** *hold-time* | **priority** *priority*] * **bidir**	缺省情况下，没有配置C-RP

3. 配置双向PIM RP的最大数目

由于双向 PIM 为每个 RP 都要在所有 PIM 接口上进行 DF 选举，因此实际组网中不建议配置多个双向 PIM RP。通过本配置可以限制双向 PIM RP 的数目，超出限制值的 RP 不会生效，仅能进行 DF 选举而无法指导转发。

提示

在配置双向 PIM RP 的最大数目时，如果现有双向 PIM RP 的数目已超过配置值，系统不会自动删除超出限制值的 RP，用户可根据需要进行手工删除。

表1-20 配置双向 PIM RP 的最大数目

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
配置双向PIM RP的最大数目	**bidir-rp-limit** *limit*	缺省情况下，双向PIM RP的最大数目为6

1.4.5 配置BSR

如果配置了静态 RP，则不需要配置 BSR；但如果配置了 C-RP 来动态选举 RP，则必须配置 BSR。在一个双向 PIM 域中只能有一个 BSR，但需要配置至少一个 C-BSR。任意一台路由器都可以被配置为 C-BSR。在 C-BSR 之间通过自动选举产生 BSR，BSR 负责在双向 PIM 域中收集并发布 RP 信息。

1. 配置C-BSR

提示

- 由于 BSR 与双向 PIM 域中的其它设备需要交换大量信息，因此应在 C-BSR 与双向 PIM 域中的其它设备之间保留较大的通信带宽。
- 当 C-BSR 与其它 PIM 路由器通过隧道连接时，如果单播路由中到 C-BSR 下一跳的不是 Tunnel 接口，请在 PIM 路由器上通过配置组播静态路由以保证这一点，否则将影响 RPF 检查。有关组播静态路由的相关配置，请参见“IP 组播配置指导”中的“组播路由与转发”。

C-BSR 应配置在骨干网的路由器上，C-BSR 间的自动选举机制简单描述如下：

- 最初，每个 C-BSR 都认为自己是本双向 PIM 域的 BSR，向其它路由器发送自举报文；
- 当某 C-BSR 收到其它 C-BSR 发来的自举报文时，首先比较自己与后者的优先级，优先级较高者获胜；在优先级相同的情况下，再比较自己与后者的 BSR 地址，拥有较大 IP 地址者获胜。如果后者获胜，则用后者的 BSR 地址替换自己的 BSR 地址，并不再认为自己是 BSR；否则，保留自己的 BSR 地址，并继续认为自己是 BSR。

在一个双向 PIM 域中，从众多 C-BSR 中选举出唯一的 BSR。双向 PIM 域内的 C-RP 向 BSR 发送宣告报文，由 BSR 汇总为 RP-Set，并向本双向 PIM 域内的所有路由器进行宣告。所有路由器都使用统一的哈希算法，得到特定组播组所对应 RP 的地址。

通过在路由器上配置合法 BSR 的地址范围，可以对收到的自举报文按照地址范围进行过滤，从而防止某些恶意主机非法伪装成 BSR，以避免合法的 BSR 被恶意取代。必须在双向 PIM 域内的所有路由器上进行相同的配置。通常针对以下两类情况实施预防措施：

- 某些恶意主机通过伪造自举报文以欺骗路由器，试图更改 RP 映射关系。这种攻击通常发生在边缘路由器上，由于 BSR 处于网络内部，主机在网络外部，因此边缘路由器通过对收到的自举报文进行邻居检查和 RPF 检查，丢弃不符合要求的报文，就可以避免外部网络用户对内部网络 BSR 的攻击；
- 网络中某台路由器被攻击者控制，或者有非法接入的路由器时，攻击者可以将这样的路由器配置为 C-BSR，并使其在竞争中获胜，从而控制网络中 RP 信息的发布权。由于在被配置为 C-BSR 后，路由器会自动向整个网络扩散自举报文，而自举报文是 TTL 值为 1 的组播报文，所以只要其邻居路由器不接收该自举报文，就不会影响整个网络。因此，通过在整个网络的所有路由器上都配置合法 BSR 的地址范围，从而丢弃合法范围之外的自举报文，就可以防止此类攻击。

以上两种预防措施可以部分地保护网络中 BSR 的安全。但是如果某台合法的 BSR 路由器被攻击者控制，还是可能导致问题。

表1-21 配置 C-BSR

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
配置C-BSR	**c-bsr** *ip-address* [**scope** *group-address* { *mask-length* | *mask* }] [**hash-length** *hash-length* | **priority** *priority*] *	缺省情况下，没有配置C-BSR
（可选）配置合法的BSR地址范围	**bsr-policy** *acl-number*	缺省情况下，BSR的地址范围不受任何限制

2. 配置BSR服务边界

BSR 作为双向 PIM 域中的管理核心，负责将收集到的 RP-Set 信息以自举报文的形式发向双向 PIM 域中的所有路由器。

BSR 的服务边界，即双向 PIM 域的边界。BSR 是针对特定的服务范围而言的，众多的 BSR 服务边界接口将网络划分成不同的双向 PIM 域，自举报文无法通过双向 PIM 域的边界，BSR 服务边界之外的路由器也不能参与本双向 PIM 域内的组播转发。

请在欲配置为 BSR 服务边界的路由器上进行如下配置。

表1-22 配置 BSR 服务边界

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置BSR的服务边界	**pim bsr-boundary**	缺省情况下，没有配置BSR的服务边界

3. 关闭自举报文语义分片功能

BSR 周期性地向所在双向 PIM 域发送自举报文以通告 RP-Set 信息。当 RP-Set 信息较少时，自举报文被封装在一个 IP 报文中发送出去；而当 RP-Set 信息较多时，自举报文的大小可能超过接口的 MTU 值，从而触发其在 IP 层的分片。在这种情况下，一个 IP 分片的丢失就会导致整个自举报文都被丢弃。

自举报文语义分片功能可以解决上述问题：当自举报文大于接口 MTU 时，会被分解为多个自举报文分片。非 BSR 收到自举报文分片后，若发现某组范围对应的 RP 信息都在这一个分片中，便立即更新该组范围对应的 RP-Set；若发现某组范围映射的 RP 信息被分在了多个分片中，则待收齐了这些分片后再更新该组范围对应的 RP-Set。这样，由于不同分片所含组范围对应的 RP 信息不同，因此个别分片的丢失只影响该分片所含组范围对应的 RP 信息，而不会导致整个自举报文都被丢弃。

自举报文语义分片功能是缺省使能的，但由于不支持该功能的设备会将自举报文分片当作完整的自举报文处理，从而导致其学到的 RP-Set 信息不完整，因此当双向 PIM 域中存在此类设备时，请在已配置为 C-BSR 的路由器上关闭本功能。

表1-23 关闭自举报文语义分片功能

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
关闭自举报文语义分片功能	**undo bsm-fragment enable**	缺省情况下，自举报文语义分片功能处于使能状态

说明

通常，BSR 根据其 BSR 接口的 MTU 值对自举报文进行语义分片；而对由于新学到 PIM 邻居而触发的自举报文发送，则根据发送接口的 MTU 值进行语义分片。

1.5 配置PIM-SSM

提示

PIM-SSM 模型需要 IGMPv3 的支持，因此应确保连接有接收者的 PIM 路由器上使能了 IGMPv3。

1.5.1 PIM-SSM配置任务简介

表1-24 PIM-SSM 配置任务简介

配置任务	说明	详细配置
使能PIM-SM	必选	1.5.3
配置SSM组播组范围	可选	1.5.4
配置PIM公共特性	可选	1.6

1.5.2 配置准备

在配置 PIM-SSM 之前，需完成以下任务：

- 配置任一单播路由协议，实现域内网络层互通

1.5.3 使能PIM-SM

提示

同一台设备相同实例的所有接口上启用的 PIM 模式必须相同。

在进行各项 PIM 配置之前，必须先使能 IP 组播路由。

由于 PIM-SSM 是通过 PIM-SM 的部分子集功能实现的，因此在配置 PIM-SSM 之前须先使能 PIM-SM。在部署 PIM-SSM 域时，建议在其所有非边界接口上均使能 PIM-SM。

表1-25 使能 PIM-SM

操作	命令	说明
进入系统视图	**system-view**	-
使能IP组播路由，并进入MRIB视图	**multicast routing** [**vpn-instance** *vpn-instance-name*]	缺省情况下，IP组播路由处于关闭状态 本命令的详细介绍请参见“IP组播命令参考”中的“组播路由与转发”
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能PIM-SM	**pim sm**	缺省情况下，PIM-SM处于关闭状态

1.5.4 配置SSM组播组范围

在把来自组播源的信息传递给接收者的过程中，是采用 PIM-SSM 模型还是 PIM-SM 模型，这取决于接收者订阅通道（S，G）中的组播组是否在 SSM 组播组范围之内，所有使能了 PIM-SM 的接口将会认为属于该范围内的组播组采用了 PIM-SSM 模型。

请在 PIM-SSM 域内的所有路由器上进行如下配置。

提示

- 应确保 PIM-SSM 域内所有路由器上配置的 SSM 组播组地址范围都一致，否则组播信息将无法通过 SSM 模型进行传输。
- 如果某组播组属于 SSM 组播组范围，但该组成员使用 IGMPv1 或 IGMPv2 发送加入报文，则设备不会触发（*，G）加入报文。

表1-26 配置 SSM 组播组范围

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim**	-
配置SSM组播组的范围	**ssm-policy** *acl-number*	缺省情况下，SSM组播组的范围为232.0.0.0/8

1.6 配置PIM公共特性

1.6.1 PIM公共特性配置任务简介

表1-27 PIM 公共特性配置任务简介

配置任务	说明	详细配置
配置组播数据过滤器	可选	1.6.3
配置Hello报文过滤器	可选	1.6.4
配置Hello报文选项	可选	1.6.5
配置PIM公共定时器	可选	1.6.6
配置加入/剪枝报文规格	可选	1.6.7
配置PIM与BFD联动	可选	1.6.8
开启PIM告警功能	可选	1.6.9

1.6.2 配置准备

在配置 PIM 公共特性之前，需完成以下任务：

- 配置任一单播路由协议，实现域内网络层互通
- 配置 PIM-DM 或 PIM-SM

1.6.3 配置组播数据过滤器

无论在 PIM-DM 还是 PIM-SM 域内，各路由器都可以对流经自己的组播数据进行检查，通过比较是否符合过滤规则来决定是否继续转发组播数据。也就是说 PIM 域内的路由器能够成为组播数据的过滤器。过滤器的存在一方面有助于实现信息流量控制，另一方面可以在安全性方面限定下游接收者能够获得的信息。过滤器不仅过滤独立的组播数据，还过滤封装在注册报文中的组播数据。

通常，过滤器的位置距离组播源越近，过滤影响越明显。

表1-28 配置组播数据过滤器

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
配置组播数据过滤器	**source-policy** *acl-number*	缺省情况下，没有配置组播数据过滤器

1.6.4 配置Hello报文过滤器

随着 PIM 协议的推广和应用，对其安全性的要求也越来越高。建立正确的 PIM 邻居是 PIM 协议安全应用的前提。如果在接口上指定了合法 Hello 报文的源地址范围，便能够保证 PIM 邻居的正确建立，从而有效防止各种 PIM 协议报文攻击，提高设备对 PIM 协议报文处理的安全性。

表1-29 配置 Hello 报文过滤器

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置合法Hello报文的源地址范围	**pim neighbor-policy** *acl-number*	缺省情况下，Hello报文的源地址范围不受任何限制

说明

当 Hello 报文过滤器的配置生效后，对于之前已建立的 PIM 邻居，若由于其 Hello 报文被过滤而导致无法收到后续的 Hello 报文，将会在老化超时后被自动删除。

1.6.5 配置Hello报文选项

无论在 PIM-DM 域还是在 PIM-SM 域内，各路由器之间发送的 Hello 报文都包含很多可供配置的选项，对各选项的介绍如下：

- DR_Priority（仅用于 PIM-SM）：表示竞选 DR 的优先级，优先级高的设备被选举为 DR。可以在与组播源或接收者直连的共享网络中的所有路由器上都配置此参数。
- Holdtime：表示保持 PIM 邻居可达状态的时间，若超时后仍没有收到 Hello 报文，则认为 PIM 邻居失效或不可达。
- LAN_Prune_Delay：表示在共享网络上传递剪枝报文的延迟时间，该选项由三部分组成：LAN-delay（发送剪枝报文的延迟时间）、Override-interval（剪枝否决时间）和禁止加入报文抑制能力。

LAN-delay 表示路由器从收到下游路由器发来的剪枝报文到继续向上游路由器发送剪枝报文的延迟时间，Override-interval 则表示允许下游路由器否决剪枝动作的时间，当共享网段内各 PIM 路由器的 LAN-delay 或 Override-interval 不同时，取其中最大的值。路由器在收到下游路由器发来的剪枝报文后并不立即执行剪枝动作，而是仍将当前的转发状态保持 LAN-delay＋Override-interval 时间。如果下游路由器需要继续接收组播数据，则必须在 Override-interval 时间内向上游路由器发送加入报文以否决这个剪枝动作，这就称为剪枝否决；如果 Override-interval 时间超时后未收到任何加入报文，上游路由器就会在 LAN-delay＋Override-interval 时间超时后执行剪枝动作。

通过在上游邻居上使能跟踪下游邻居的功能（即关闭加入报文抑制能力），可以记录已发送了加入报文且加入状态尚未超时的下游邻居的信息。使能该功能时，应在共享网段的所有 PIM 路由器上都使能，否则上游邻居无法跟踪每个下游邻居的加入报文。

在接口上使能 PIM 后，路由器会生成一个随机数作为 Hello 报文中的 Generation ID。一台 PIM 路由器的 Generation ID 一般不会改变，除非其状态更新才会生成新的 Generation ID。这样，当 PIM 路由器发现来自上游邻居的 Hello 报文中的 Generation ID 发生改变时，便认为上游邻居的状态发生了改变，从而触发发送加入报文以进行状态刷新。通过在接口上配置拒绝无 Generation ID 的 Hello 报文，可以实时了解上游邻居的状态。

对于既可在 PIM 视图又可在接口视图下进行的配置来说，前者对所有接口都生效，而后者只对当前接口生效，但后者的配置优先级较高。

1. 全局配置Hello报文选项

表1-30 全局配置 Hello 报文选项

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
配置竞选DR的优先级	**hello-option dr-priority** *priority*	缺省情况下，竞选DR的优先级为1
配置保持PIM邻居可达状态的时间	**hello-option holdtime** *time*	缺省情况下，保持PIM邻居可达状态的时间为105秒
配置发送剪枝报文的延迟时间	**hello-option lan-delay** *delay*	缺省情况下，发送剪枝报文的延迟时间为500毫秒
配置剪枝否决时间	**hello-option override-interval** *interval*	缺省情况下，剪枝否决时间为2500毫秒
使能邻居跟踪功能	**hello-option neighbor-tracking**	缺省情况下，邻居跟踪功能处于关闭状态

2. 在接口上配置Hello报文选项

表1-31 在接口上配置 Hello 报文选项

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置竞选DR的优先级	**pim hello-option dr-priority** *priority*	缺省情况下，竞选DR的优先级为1
配置保持PIM邻居可达状态的时间	**pim hello-option holdtime** *time*	缺省情况下，保持PIM邻居可达状态的时间为105秒
配置发送剪枝报文的延迟时间	**pim hello-option lan-delay** *delay*	缺省情况下，发送剪枝报文的延迟时间为500毫秒
配置剪枝否决时间	**pim hello-option override-interval** *interval*	缺省情况下，剪枝否决时间为2500毫秒
使能邻居跟踪功能	**pim hello-option neighbor-tracking**	缺省情况下，邻居跟踪功能处于关闭状态
配置拒绝无Generation ID的Hello报文	**pim require-genid**	缺省情况下，接受无Generation ID的Hello报文

1.6.6 配置PIM公共定时器

提示

- 如果对网络没有特殊要求，各定时器的值建议采用缺省值。
- PIM 接口向上游邻居发送加入/剪枝报文的时间间隔必须小于加入/剪枝状态的保持时间，以免上游邻居老化超时。

PIM 路由器通过周期性地发送 Hello 报文，以发现 PIM 邻居，并维护各路由器之间的 PIM 邻居关系。

为了避免多个 PIM 路由器同时发送 Hello 报文而导致冲突，当 PIM 路由器在收到新邻居发来的 Hello 报文时，将延迟一段时间再发送 Hello 报文，该时间值为小于“触发 Hello 报文的最大延迟时间”的一个随机值。

PIM 路由器通过周期性地向其上游路由器发送加入/剪枝报文以更新状态，在该报文中携带有保持时间，上游路由器为被剪枝的下游接口设置加入/剪枝状态保持定时器。

当路由器没有收到来自组播源 S 的后续组播数据时，不会立即删除（S，G）表项，而是将其维持一段时间后再删除，这段时间就称为组播源的生存时间。

对于既可在 PIM 视图又可在接口视图下进行的配置来说，前者对所有接口都生效，而后者只对当前接口生效，但后者的配置优先级较高。

1. 全局配置PIM公共定时器

表1-32 全局配置 PIM 公共定时器

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
配置发送Hello报文的时间间隔	**timer hello** *interval*	缺省情况下，发送Hello报文的时间间隔为30秒
配置发送加入/剪枝报文的时间间隔	**timer join-prune** *interval*	缺省情况下，发送加入/剪枝报文的时间间隔为60秒 本命令不会立即生效，新配置的发送间隔将在当前发送间隔完成后生效
配置加入/剪枝状态的保持时间	**holdtime join-prune** *time*	缺省情况下，加入/剪枝状态的保持时间为210秒
配置组播源生存时间	**source-lifetime** *time*	缺省情况下，组播源的生存时间为210秒

2. 在接口上配置PIM公共定时器

表1-33 在接口上配置 PIM 公共定时器

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入接口视图	**interface** *interface-type interface-number*	-
配置发送Hello报文的时间间隔	**pim timer hello** *interval*	缺省情况下，发送Hello报文的时间间隔为30秒
配置触发Hello报文的最大延迟时间	**pim triggered-hello-delay** *delay*	缺省情况下，触发Hello报文的最大延迟时间为5秒
配置发送加入/剪枝报文的时间间隔	**pim timer join-prune** *interval*	缺省情况下，发送加入/剪枝报文的时间间隔为60秒 本命令不会立即生效，新配置的发送间隔将在当前发送间隔完成后生效
配置加入/剪枝状态的保持时间	**pim holdtime join-prune** *time*	缺省情况下，加入/剪枝状态的保持时间为210秒

1.6.7 配置加入/剪枝报文规格

如果加入/剪枝报文的尺寸较大，则丢失一个报文将导致较多信息的遗失；如果加入/剪枝报文的尺寸较小，则单个报文的丢失所产生的影响也将降低。

表1-34 配置加入/剪枝报文规格

操作	命令	说明
进入系统视图	**system-view**	-
进入PIM视图	**pim** [**vpn-instance** *vpn-instance-name*]	-
配置加入/剪枝报文的最大长度	**jp-pkt-size** *size*	缺省情况下，加入/剪枝报文的最大长度为8100字节

1.6.8 配置PIM与BFD联动

提示

只有在接口上先使能了 PIM-DM 或 PIM-SM，本配置才能生效。

PIM 借助 Hello 报文在共享网段中选举出 DR，使其成为该网段中组播数据的唯一转发者。当 DR 出现故障时，只有待其老化后才会触发新的 DR 选举过程，这个过程通常比较长。为了实现 DR 的快速切换，可以在共享网段的 PIM 邻居之间引入 BFD（Bidirectional Forwarding Detection，双向转发检测）机制进行链路状态的快速检测。通过在共享网段内的所有 PIM 路由器上都使能 PIM 与 BFD 联动功能，可以使这些 PIM 邻居快速感知 DR 故障并重新选举 DR。有关 BFD 的详细介绍，请参见“可靠性配置指导”中的“BFD”。

表1-35 配置 PIM 与 BFD 联动

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能PIM与BFD联动功能	**pim bfd enable**	缺省情况下，PIM与BFD联动功能处于关闭状态

1.6.9 开启PIM告警功能

开启了 PIM 的告警功能之后，PIM 会生成告警信息，以向网管软件报告本模块的重要事件。该信息将发送至 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

表1-36 开启 PIM 告警功能

操作	命令	说明
进入系统视图	**system-view**	-
开启PIM的告警功能	**snmp-agent trap enable pim** [**candidate-bsr-win-election** | **elected-bsr-lost-election** | **neighbor-loss**] *	缺省情况下，PIM的告警功能处于开启状态

1.7 PIM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 的运行情况，通过查看显示信息验证配置的效果。

表1-37 PIM 显示和维护

操作	命令
显示Register-Tunnel接口的相关信息	**display interface** [**register-tunnel** [*interface-number*]] [**brief** [**description** | **down**]]
显示PIM-SM域中的BSR信息	**display pim** [**vpn-instance** *vpn-instance-name*] **bsr-info**
显示PIM所使用的路由信息	**display pim** [**vpn-instance** *vpn-instance-name*] **claimed-route** [*source-address*]
显示PIM-SM域中的C-RP信息	**display pim** [**vpn-instance** *vpn-instance-name*] **c-rp** [**local**]
显示双向PIM的DF信息	**display pim** [**vpn-instance** *vpn-instance-name*] **df-info** [*rp-address*]
显示接口上的PIM信息	**display pim** [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**verbose**]
显示PIM邻居信息	**display pim** [**vpn-instance** *vpn-instance-name*] **neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *

操作	命令
显示PIM路由表的内容	**display pim** [**vpn-instance** *vpn-instance-name*] **routing-table** [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **flags** *flag-value* | **fsm** | **incoming-interface** *interface-type interface-number* | **mode** *mode-type* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *
显示PIM-SM域中的RP信息	**display pim** [**vpn-instance** *vpn-instance-name*] **rp-info** [*group-address*]
显示PIM协议报文的统计信息	**display pim statistics**

1.8 PIM典型配置举例

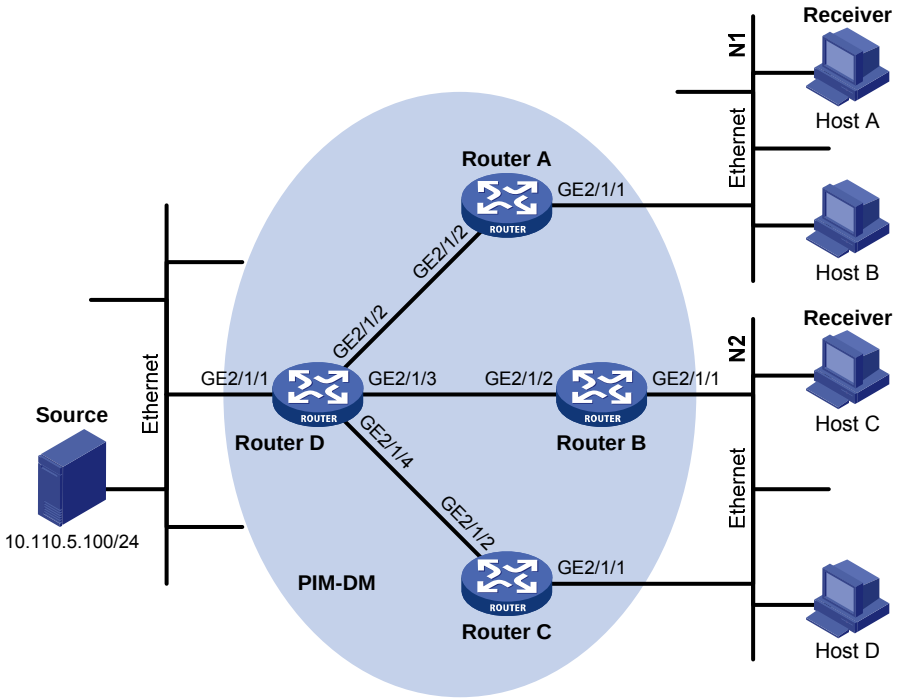
1.8.1 PIM-DM典型配置举例

1. 组网需求

- 接收者通过组播方式接收视频点播信息，不同组织的接收者群体组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 PIM 域采用 DM 方式。
- Host A 和 Host C 为两个末梢网络中的组播信息接收者；Router D 通过 GigabitEthernet2/1/1 接口与组播源（Source）所在的网络连接；Router A 通过 GigabitEthernet2/1/1 接口连接末梢网络 N1，通过 GigabitEthernet2/1/2 接口连接 Router D；Router B 和 Router C 分别通过各自的 GigabitEthernet2/1/1 接口连接末梢网络 N2，并分别通过各自的 GigabitEthernet2/1/2 接口连接 Router D。
- Router A 与末梢网络 N1 之间运行 IGMPv2；Router B 和 Router C 与末梢网络 N2 之间也运行 IGMPv2。

2. 组网图

图1-15 PIM-DM 典型配置组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	GE2/1/1	10.110.1.1/24	Router D	GE2/1/1	10.110.5.1/24
	GE2/1/2	192.168.1.1/24		GE2/1/2	192.168.1.2/24
Router B	GE2/1/1	10.110.2.1/24		GE2/1/3	192.168.2.2/24
	GE2/1/2	192.168.2.1/24		GE2/1/4	192.168.3.2/24
Router C	GE2/1/1	10.110.2.2/24			
	GE2/1/2	192.168.3.1/24			

3. 配置步骤

(1) 配置 IP 地址和单播路由协议

请按照 图 1-15 配置各接口的IP地址和子网掩码，具体配置过程略。

配置 PIM-DM 域内的各路由器之间采用 OSPF 协议进行互连，确保 PIM-DM 域内部在网络层互通，并且各路由器之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，并使能 PIM-DM 和 IGMP

在 Router A 上使能 IP 组播路由，在接口 GigabitEthernet2/1/2 上使能 PIM-DM，并在其连接末梢网络的接口 GigabitEthernet2/1/1 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] igmp enable
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] pim dm
[RouterA-GigabitEthernet2/1/2] quit
```

Router B 和 Router C 的配置与 Router A 相似，配置过程略。

在 Router D 上使能 IP 组播路由，并在各接口上使能 PIM-DM。

```
<RouterD> system-view
[RouterD] multicast routing
[RouterD-mrib] quit
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] pim dm
[RouterD-GigabitEthernet2/1/1] quit
[RouterD] interface gigabitethernet 2/1/2
[RouterD-GigabitEthernet2/1/2] pim dm
[RouterD-GigabitEthernet2/1/2] quit
[RouterD] interface gigabitethernet 2/1/3
[RouterD-GigabitEthernet2/1/3] pim dm
[RouterD-GigabitEthernet2/1/3] quit
[RouterD] interface gigabitethernet 2/1/4
[RouterD-GigabitEthernet2/1/4] pim dm
[RouterD-GigabitEthernet2/1/4] quit
```

4. 验证配置

通过使用 **display pim interface** 命令可以查看路由器接口上 PIM 的配置和运行情况。例如：

显示 Router D 上 PIM 的配置信息。

```
[RouterD] display pim interface
 Interface           NbrCnt HelloInt   DR-Pri     DR-Address
 GE2/1/1             0      30         1          10.110.5.1     (local)
 GE2/1/2             1      30         1          192.168.1.2    (local)
 GE2/1/3             1      30         1          192.168.2.2    (local)
 GE2/1/4             1      30         1          192.168.3.2    (local)
```

通过使用 **display pim neighbor** 命令可以显示路由器之间的 PIM 邻居关系。例如：

显示 Router D 上 PIM 的邻居关系信息。

```
[RouterD] display pim neighbor
 Total Number of Neighbors = 3

 Neighbor         Interface           Uptime   Expires  Dr-Priority
 192.168.1.1      GE2/1/2             00:02:22 00:01:27 1
 192.168.2.1      GE2/1/3             00:00:22 00:01:29 3
 192.168.3.1      GE2/1/4             00:00:23 00:01:31 5
```

假如 Host A 需要接收组播组 G（225.1.1.1）的信息，当组播源 S（10.110.5.100/24）向组播组 G 发送组播数据时，通过扩散生成 SPT，SPT 路径中各路由器（Router A 和 Router D）上都存在（S，G）表项，Host A 向 Router A 发送 IGMP 报告以加入组播组 G，在 Router A 上生成（*，G）表项。

通过使用 **display pim routing-table** 命令可以查看路由器的 PIM 路由表信息。例如：

显示 Router A 上的 PIM 路由表信息。

```
[RouterA] display pim routing-table
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 225.1.1.1)
     Protocol: pim-dm, Flag: WC
```

```
    UpTime: 00:04:25
    Upstream interface: NULL
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/1/1
            Protocol: igmp, UpTime: 00:04:25, Expires: -

 (10.110.5.100, 225.1.1.1)
    Protocol: pim-dm, Flag: ACT
    UpTime: 00:06:14
    Upstream interface: GigabitEthernet2/1/2
        Upstream neighbor: 192.168.1.2
        RPF prime neighbor: 192.168.1.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/1/1
            Protocol: pim-dm, UpTime: 00:04:25, Expires: -
```

显示 Router D 上的 PIM 路由表信息。

```
[RouterD] display pim routing-table
 Total 0 (*, G) entry; 1 (S, G) entry

 (10.110.5.100, 225.1.1.1)
    Protocol: pim-dm, Flag: LOC ACT
    UpTime: 00:03:27
    Upstream interface: GigabitEthernet2/1/1
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 2
        1: GigabitEthernet2/1/2
            Protocol: pim-dm, UpTime: 00:03:27, Expires: -
        2: GigabitEthernet2/1/4
            Protocol: pim-dm, UpTime: 00:03:27, Expires: -
```

1.8.2 PIM-SM非管理域配置举例

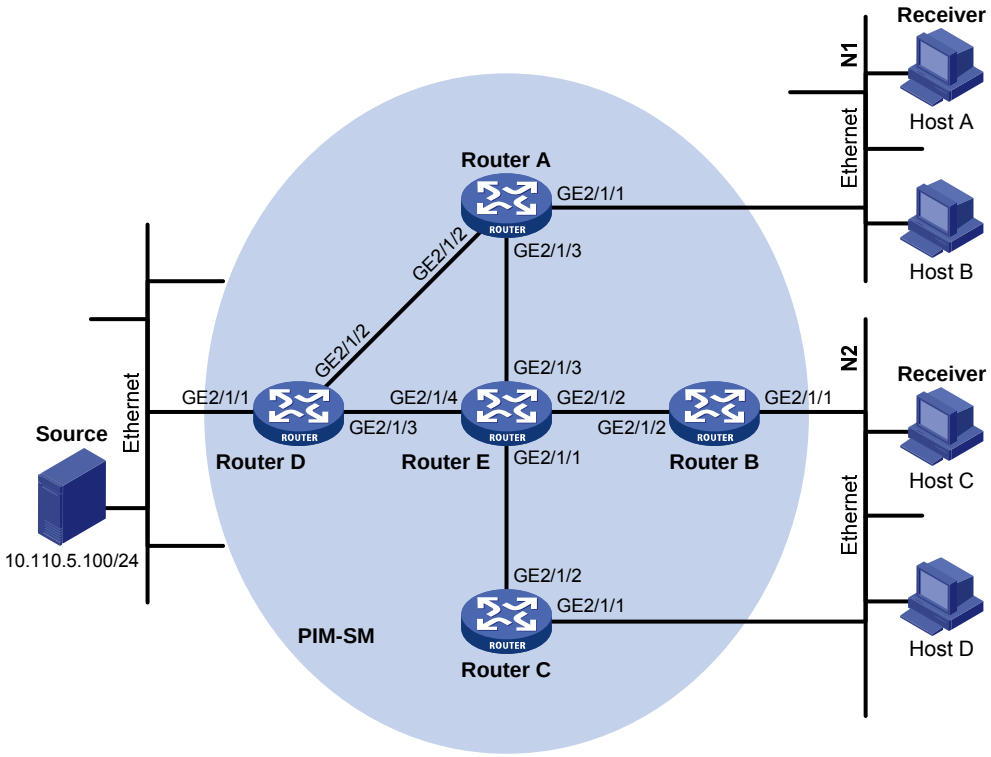
1. 组网需求

- 接收者通过组播方式接收视频点播信息，不同组织的接收者群体组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 PIM 域采用 SM 非管理域方式。
- Host A 和 Host C 为两个末梢网络中的组播信息接收者；Router D 通过 GigabitEthernet2/1/1 接口与组播源（Source）所在网络连接；Router A 通过 GigabitEthernet2/1/1 接口连接末梢网络 N1，通过 GigabitEthernet2/1/2 接口和 GigabitEthernet2/1/3 接口分别连接 Router D 和 Router E；Router B 和 Router C 分别通过各自的 GigabitEthernet2/1/1 接口连接末梢网络 N2，并分别通过各自的 GigabitEthernet2/1/2 接口连接 Router E。

- 将 Router E 的 GigabitEthernet2/1/3 接口配置为 C-BSR 和 C-RP，其中 C-RP 所服务的组播组范围为 225.1.1.0/24；在所有路由器上将 Router D 的 GigabitEthernet2/1/2 接口配置为静态 RP，以对动态 RP 进行备份。
- Router A 与末梢网络 N1 之间运行 IGMPv2；Router B 和 Router C 与末梢网络 N2 之间也运行 IGMPv2。

2. 组网图

图1-16 PIM-SM 非管理域配置组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	GE2/1/1	10.110.1.1/24	Router D	GE2/1/1	10.110.5.1/24
	GE2/1/2	192.168.1.1/24		GE2/1/2	192.168.1.2/24
	GE2/1/3	192.168.9.1/24		GE2/1/3	192.168.4.2/24
Router B	GE2/1/1	10.110.2.1/24	Router E	GE2/1/1	192.168.3.2/24
	GE2/1/2	192.168.2.1/24		GE2/1/2	192.168.2.2/24
Router C	GE2/1/1	10.110.2.2/24		GE2/1/3	192.168.9.2/24
	GE2/1/2	192.168.3.1/24		GE2/1/4	192.168.4.1/24

3. 配置步骤

(1) 配置 IP 地址和单播路由协议

请按照 图 1-16 配置各接口的IP地址和子网掩码，具体配置过程略。

配置 PIM-SM 域内的各路由器之间采用 OSPF 协议进行互连，确保 PIM-SM 域内部在网络层互通，并且各路由器之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，并使能 PIM-SM 和 IGMP

在 Router A 上使能 IP 组播路由，在其连接末梢网络的接口 GigabitEthernet2/1/1 上使能 IGMP，并在其它接口上使能 PIM-SM。

```
<RouterA> system-view
```

```
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] igmp enable
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] pim sm
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] interface gigabitethernet 2/1/3
[RouterA-GigabitEthernet2/1/3] pim sm
[RouterA-GigabitEthernet2/1/3] quit
```

Router B 和 Router C 的配置与 Router A 相似，Router D 和 Router E 除了不需要在相应接口上使能 IGMP 外，其它的配置也与 Router A 相似，配置过程略。

(3) 配置 C-BSR、C-RP 和静态 RP

在 Router E 上配置 RP 通告的服务范围，以及 C-BSR 和 C-RP 的位置，并指定静态 RP。

```
<RouterE> system-view
[RouterE] acl number 2005
[RouterE-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[RouterE-acl-basic-2005] quit
[RouterE] pim
[RouterE-pim] c-bsr 192.168.9.2
[RouterE-pim] c-rp 192.168.9.2 group-policy 2005
[RouterE-pim] static-rp 192.168.1.2
[RouterE-pim] quit
```

在 Router A 上配置静态 RP。

```
[RouterA] pim
[RouterA-pim] static-rp 192.168.1.2
[RouterA-pim] quit
```

Router B、Router C 和 Router D 的配置与 Router A 相似，配置过程略。

4. 验证配置

通过使用 **display pim interface** 命令可以查看接口上的 PIM 信息。例如：

显示 Router A 的接口上的 PIM 信息。

```
[RouterA] display pim interface
 Interface           NbrCnt HelloInt   DR-Pri     DR-Address
 GE2/1/1             0      30         1          10.110.1.1     (local)
 GE2/1/2             1      30         1          192.168.1.2
 GE2/1/3             1      30         1          192.168.9.2
```

通过使用 **display pim bsr-info** 命令可以查看 PIM-SM 域中的 BSR 信息。例如：

显示 Router A 上 PIM-SM 域中的 BSR 信息。

```
[RouterA] display pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:44
     Elected BSR address: 192.168.9.2
       Priority: 64
```

```
    Hash mask length: 30
    Uptime: 00:11:18
```

显示 Router E 上 PIM-SM 域中的 BSR 信息。

```
[RouterE] display pim bsr-info
 Scope: non-scoped
     State: Elected
     Bootstrap timer: 00:01:44
     Elected BSR address: 192.168.9.2
       Priority: 64
       Hash mask length: 30
       Uptime: 00:11:18
     Candidate BSR address: 192.168.9.2
       Priority: 64
       Hash mask length: 30
```

通过使用 **display pim rp-info** 命令可以查看 PIM-SM 域中的 RP 信息。例如：

显示 Router A 上所有组播组对应的 RP 信息。

```
[RouterA] display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 225.1.1.0/24
       RP address               Priority  HoldTime  Uptime    Expires
       192.168.9.2              192       150       00:51:45  00:02:22

 Static RP information:
       RP address               ACL   Mode    Preferred
       192.168.1.2              ----  pim-sm  No
```

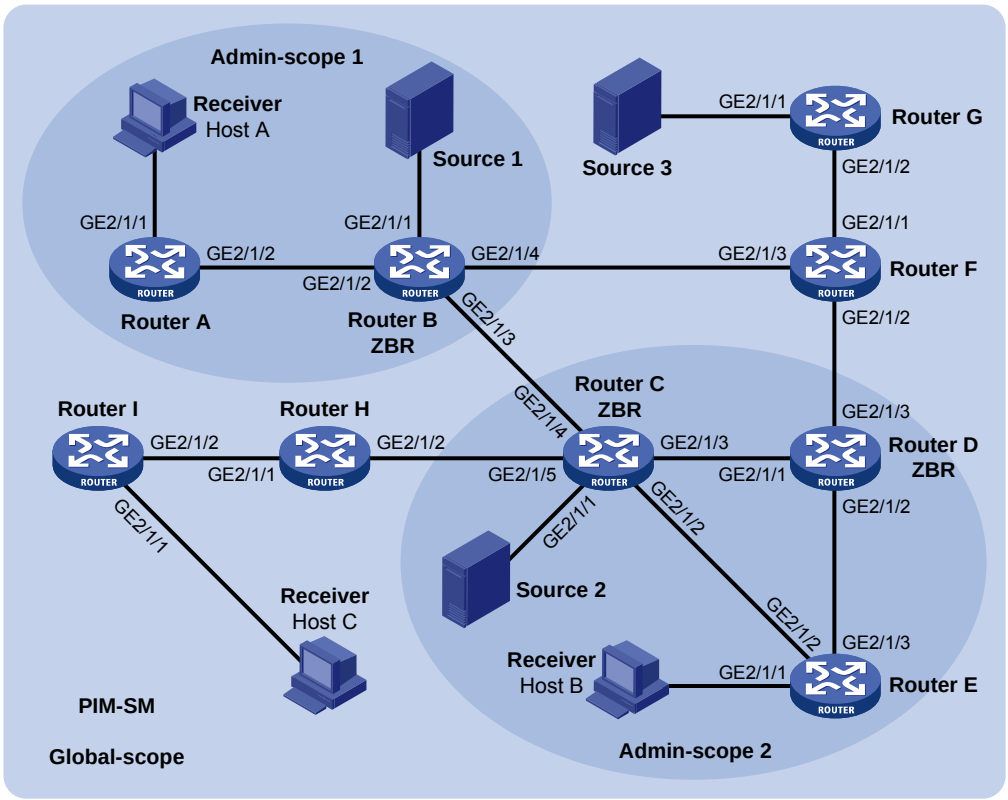
1.8.3 PIM-SM管理域配置举例

1. 组网需求

- 接收者通过组播方式接收视频点播信息，整个PIM域采用SM管理域方式，划分为管理域1、管理域 2 和 Global 域，Router B、Router C 和 Router D 为各管理域的 ZBR。
- Source 1 和 Source 2 分别向组播组 239.1.1.1 发送内容不同的组播信息，Host A 和 Host B 则分别只接收来自 Source 1 和 Source 2 的组播信息；Source 3 向组播组 224.1.1.1 发送组播信息，Host C 为其接收者。
- Router B 的 GigabitEthernet2/1/2 接口为管理域 1 的 C-BSR 和 C-RP，服务于 239.0.0.0/8；Router D 的 GigabitEthernet2/1/1 接口为管理域 2 的 C-BSR 和 C-RP，服务于 239.0.0.0/8；Router F 的 GigabitEthernet2/1/1 接口为 Global 域的 C-BSR 和 C-RP，服务于 239.0.0.0/8 以外的所有组播组。
- Router A、Router E 和 Router I 分别与各自所连接的接收者之间运行 IGMPv2。

2. 组网图

图1-17 PIM-SM 管理域配置组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	GE2/1/1	192.168.1.1/24	Router D	GE2/1/1	10.110.5.2/24
	GE2/1/2	10.110.1.1/24		GE2/1/2	10.110.7.1/24
Router B	GE2/1/1	192.168.2.1/24		GE2/1/3	10.110.8.1/24
	GE2/1/2	10.110.1.2/24	Router E	GE2/1/1	192.168.4.1/24
	GE2/1/3	10.110.2.1/24		GE2/1/2	10.110.4.2/24
	GE2/1/4	10.110.3.1/24		GE2/1/3	10.110.7.2/24
Router C	GE2/1/1	192.168.3.1/24	Router F	GE2/1/1	10.110.9.1/24
	GE2/1/2	10.110.4.1/24		GE2/1/2	10.110.8.2/24
	GE2/1/3	10.110.5.1/24		GE2/1/3	10.110.3.2/24
	GE2/1/4	10.110.2.2/24	Router G	GE2/1/1	192.168.5.1/24
	GE2/1/5	10.110.6.1/24		GE2/1/2	10.110.9.2/24
Router H	GE2/1/1	10.110.10.1/24	Source 1	-	192.168.2.10/24
	GE2/1/2	10.110.6.2/24	Source 2	-	192.168.3.10/24
Router I	GE2/1/1	192.168.6.1/24	Source 3	-	192.168.5.10/24
	GE2/1/2	10.110.10.2/24			

3. 配置步骤

(1) 配置 IP 地址和单播路由协议

请按照 图 1-17 配置各接口的IP地址和子网掩码，具体配置过程略。

配置 PIM-SM 域内的各路由器之间采用 OSPF 协议进行互连，确保 PIM-SM 域内部在网络层互通，并且各路由器之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，并使能 PIM-SM 和 IGMP

在 Router A 上使能 IP 组播路由，在接口 GigabitEthernet2/1/2 上使能 PIM-SM，并在其连接有接收者的接口 GigabitEthernet2/1/1 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] igmp enable
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] pim sm
[RouterA-GigabitEthernet2/1/2] quit
```

Router E 和 Router I 的配置与 Router A 相似，配置过程略。

在 Router B 上使能 IP 组播路由，并在各接口上使能 PIM-SM。

```
<RouterB> system-view
[RouterB] multicast routing
[RouterB-mrib] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] pim sm
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] pim sm
[RouterB-GigabitEthernet2/1/2] quit
[RouterB] interface gigabitethernet 2/1/3
[RouterB-GigabitEthernet2/1/3] pim sm
[RouterB-GigabitEthernet2/1/3] quit
[RouterB] interface gigabitethernet 2/1/4
[RouterB-GigabitEthernet2/1/4] pim sm
[RouterB-GigabitEthernet2/1/4] quit
```

Router C、Router D、Router F、Router G 和 Router H 的配置与 Router B 相似，配置过程略。

(3) 配置管理域边界

在 Router B 上将接口 GigabitEthernet2/1/3 和 GigabitEthernet2/1/4 配置为管理域 1 的边界。

```
[RouterB] interface gigabitethernet 2/1/3
[RouterB-GigabitEthernet2/1/3] multicast boundary 239.0.0.0 8
[RouterB-GigabitEthernet2/1/3] quit
[RouterB] interface gigabitethernet 2/1/4
[RouterB-GigabitEthernet2/1/4] multicast boundary 239.0.0.0 8
[RouterB-GigabitEthernet2/1/4] quit
```

在 Router C 上将接口 GigabitEthernet2/1/4 和 GigabitEthernet2/1/5 配置为管理域 2 的边界。

```
<RouterC> system-view
[RouterC] interface gigabitethernet 2/1/4
[RouterC-GigabitEthernet2/1/4] multicast boundary 239.0.0.0 8
[RouterC-GigabitEthernet2/1/4] quit
[RouterC] interface gigabitethernet 2/1/5
[RouterC-GigabitEthernet2/1/5] multicast boundary 239.0.0.0 8
[RouterC-GigabitEthernet2/1/5] quit
```

在 Router D 上将接口 GigabitEthernet2/1/3 配置为管理域 2 的边界。

```
<RouterD> system-view
[RouterD] interface gigabitethernet 2/1/3
[RouterD-GigabitEthernet2/1/3] multicast boundary 239.0.0.0 8
[RouterD-GigabitEthernet2/1/3] quit
```

(4) 配置 C-BSR 和 C-RP

在 Router B 上配置 RP 通告的服务范围，并将接口 GigabitEthernet2/1/2 配置为管理域 1 的 C-BSR 和 C-RP。

```
[RouterB] acl number 2001
[RouterB-acl-basic-2001] rule permit source 239.0.0.0 0.255.255.255
[RouterB-acl-basic-2001] quit
[RouterB] pim
[RouterB-pim] c-bsr 10.110.1.2 scope 239.0.0.0 8
[RouterB-pim] c-rp 10.110.1.2 group-policy 2001
[RouterB-pim] quit
```

在 Router D 上配置 RP 通告的服务范围，并将接口 GigabitEthernet2/1/1 配置为管理域 2 的 C-BSR 和 C-RP。

```
[RouterD] acl number 2001
[RouterD-acl-basic-2001] rule permit source 239.0.0.0 0.255.255.255
[RouterD-acl-basic-2001] quit
[RouterD] pim
[RouterD-pim] c-bsr 10.110.5.2 scope 239.0.0.0 8
[RouterD-pim] c-rp 10.110.5.2 group-policy 2001
[RouterD-pim] quit
```

在 Router F 上将接口 GigabitEthernet2/1/1 配置为 Global 域的 C-BSR 和 C-RP。

```
<RouterF> system-view
[RouterF] pim
[RouterF-pim] c-bsr 10.110.9.1
[RouterF-pim] c-rp 10.110.9.1
[RouterF-pim] quit
```

4. 验证配置

通过使用 **display pim bsr-info** 命令可以查看 PIM-SM 域中的 BSR 信息。例如：

显示 Router B 上 PIM-SM 域中的 BSR 信息。

```
[RouterB] display pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:44
     Elected BSR address: 10.110.9.1
       Priority: 64
       Hash mask length: 30
       Uptime: 00:01:45

 Scope: 239.0.0.0/8
     State: Elected
     Bootstrap timer: 00:00:06
     Elected BSR address: 10.110.1.2
```

```
    Priority: 64
    Hash mask length: 30
    Uptime: 00:04:54
  Candidate BSR address: 10.110.1.2
    Priority: 64
    Hash mask length: 30
```

显示 Router D 上 PIM-SM 域中的 BSR 信息。

```
[RouterD] display pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:44
     Elected BSR address: 10.110.9.1
       Priority: 64
       Hash mask length: 30
       Uptime: 00:01:45

 Scope: 239.0.0.0/8
     State: Elected
     Bootstrap timer: 00:01:12
     Elected BSR address: 10.110.5.2
       Priority: 64
       Hash mask length: 30
       Uptime: 00:03:48
     Candidate BSR address: 10.110.5.2
       Priority: 64
       Hash mask length: 30
```

显示 Router F 上 PIM-SM 域中的 BSR 信息。

```
[RouterF] display pim bsr-info
 Scope: non-scoped
     State: Elected
     Bootstrap timer: 00:00:49
     Elected BSR address: 10.110.9.1
       Priority: 64
       Hash mask length: 30
       Uptime: 00:11:11
     Candidate BSR address: 10.110.9.1
       Priority: 64
       Hash mask length: 30
```

通过使用 **display pim rp-info** 命令可以查看 PIM-SM 域中的 RP 信息。例如：

显示 Router B 上所有组播组对应的 RP 信息。

```
[RouterB] display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4
       RP address               Priority  HoldTime  Uptime    Expires
       10.110.9.1               192       150       00:03:39  00:01:51
   Scope: 239.0.0.0/8
```

```
    Group/MaskLen: 239.0.0.0/8
      RP address               Priority  HoldTime  Uptime    Expires
      10.110.1.2 (local)       192       150       00:07:44  00:01:51
```

显示 Router D 上所有组播组对应的 RP 信息。

```
[RouterD] display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4
       RP address               Priority  HoldTime  Uptime    Expires
       10.110.9.1               192       150       00:03:42  00:01:48
   Scope: 239.0.0.0/8
     Group/MaskLen: 239.0.0.0/8
       RP address               Priority  HoldTime  Uptime    Expires
       10.110.5.2 (local)       192       150       00:06:54  00:02:41
```

显示 Router F 上所有组播组对应的 RP 信息。

```
[RouterF] display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4
       RP address               Priority  HoldTime  Uptime    Expires
       10.110.9.1 (local)       192       150       00:00:32  00:01:58
```

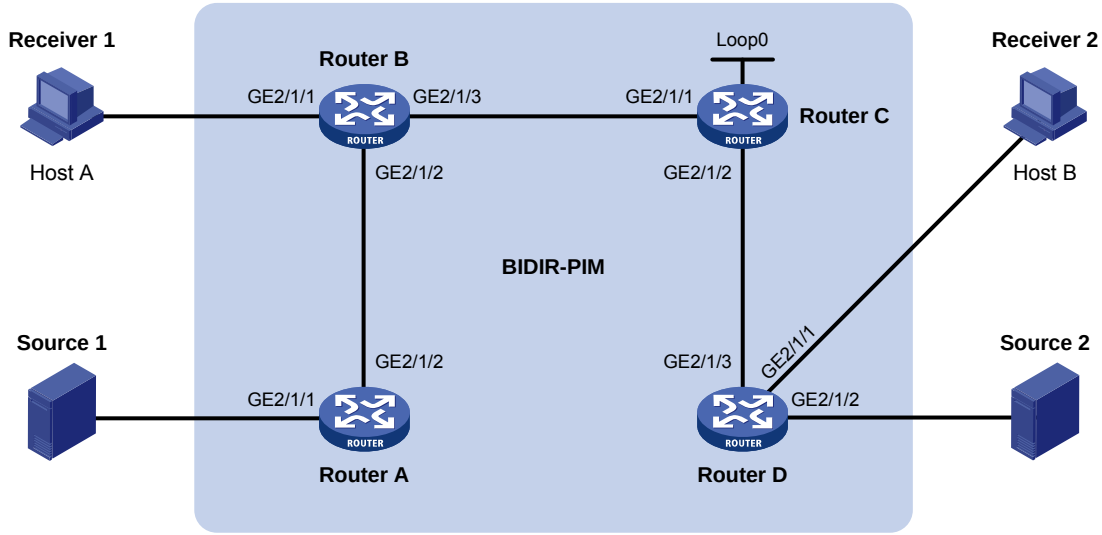
1.8.4 双向PIM典型配置举例

1. 组网需求

- 整个 PIM 域采用 BIDIR 方式，Source 1 和 Source 2 都向组播组 225.1.1.1 发送组播信息，Host A 和 Host B 为组播信息的接收者。
- 将 Router C 的 GigabitEthernet2/1/1 接口配置为 C-BSR，Loopback0 接口配置为服务于双向 PIM 的 C-RP。
- Router B 和 Router D 分别与各自所连接的接收者之间运行 IGMPv2。

2. 组网图

图1-18 双向 PIM 典型配置组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	GE2/1/1	192.168.1.1/24	Router D	GE2/1/1	192.168.3.1/24
	GE2/1/2	10.110.1.1/24		GE2/1/2	192.168.4.1/24
Router B	GE2/1/1	192.168.2.1/24		GE2/1/3	10.110.3.2/24
	GE2/1/2	10.110.1.2/24	Source 1	-	192.168.1.100/24
	GE2/1/3	10.110.2.1/24	Source 2	-	192.168.4.100/24
Router C	GE2/1/1	10.110.2.2/24	Receiver 1	-	192.168.2.100/24
	GE2/1/2	10.110.3.1/24	Receiver 2	-	192.168.3.100/24
	Loop0	1.1.1.1/32			

3. 配置步骤

(1) 配置 IP 地址和单播路由协议

请按照 图 1-18 配置各接口的IP地址和子网掩码，具体配置过程略。

配置双向 PIM 域内的各路由器之间采用 OSPF 协议进行互连，确保双向 PIM 域内部在网络层互通，并且各路由器之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，并使能 PIM-SM、双向 PIM 和 IGMP

在 Router A 上使能 IP 组播路由，在各接口上使能 PIM-SM，并使能双向 PIM。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] pim sm
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] pim sm
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] pim
[RouterA-pim] bidir-pim enable
[RouterA-pim] quit
```

在 Router B 上使能 IP 组播路由，在其连接有接收者的接口 GigabitEthernet2/1/1 上使能 IGMP，在其它接口上使能 PIM-SM，并使能双向 PIM。

```
<RouterB> system-view
[RouterB] multicast routing
[RouterB-mrib] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] igmp enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] pim sm
[RouterB-GigabitEthernet2/1/2] quit
[RouterB] interface gigabitethernet 2/1/3
[RouterB-GigabitEthernet2/1/3] pim sm
[RouterB-GigabitEthernet2/1/3] quit
[RouterB] pim
[RouterB-pim] bidir-pim enable
[RouterB-pim] quit
```

在 Router C 上使能 IP 组播路由，在各接口上使能 PIM-SM，并使能双向 PIM。

```
<RouterC> system-view
[RouterC] multicast routing
[RouterC-mrib] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] pim sm
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface gigabitethernet 2/1/2
[RouterC-GigabitEthernet2/1/2] pim sm
[RouterC-GigabitEthernet2/1/2] quit
[RouterC] interface loopback 0
[RouterC-LoopBack0] pim sm
[RouterC-LoopBack0] quit
[RouterC] pim
[RouterC-pim] bidir-pim enable
```

在 Router D 上使能 IP 组播路由，在其连接有接收者的接口 GigabitEthernet2/1/1 上使能 IGMP，在其它接口上使能 PIM-SM，并使能双向 PIM。

```
<RouterD> system-view
[RouterD] multicast routing
[RouterD-mrib] quit
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] igmp enable
[RouterD-GigabitEthernet2/1/1] quit
[RouterD] interface gigabitethernet 2/1/2
[RouterD-GigabitEthernet2/1/2] pim sm
[RouterD-GigabitEthernet2/1/2] quit
[RouterD] interface gigabitethernet 2/1/3
[RouterD-GigabitEthernet2/1/3] pim sm
[RouterD-GigabitEthernet2/1/3] quit
[RouterD] pim
```

```
[RouterD-pim] bidir-pim enable
[RouterD-pim] quit
```

(3) 配置 C-BSR 和 C-RP

在 Router C 上将接口 GigabitEthernet2/1/1 配置为 C-BSR，并将接口 Loopback0 配置为服务于双向 PIM 的 C-RP。

```
[RouterC-pim] c-bsr 10.110.2.2
[RouterC-pim] c-rp 1.1.1.1 bidir
[RouterC-pim] quit
```

4. 验证配置效果

通过使用 **display pim df-info** 命令可以查看路由器上双向 PIM 的 DF 信息。例如：

显示 Router A 上双向 PIM 的 DF 信息。

```
[RouterA] display pim df-info
 RP address: 1.1.1.1
  Interface           State   DF-Pref    DF-Metric  DF-Uptime DF-Address
  GE2/1/1             Win     100        2          01:08:50  192.168.1.1 (local)
  GE2/1/2             Lose    100        1          01:07:49  10.110.1.2
```

显示 Router B 上双向 PIM 的 DF 信息。

```
[RouterB] display pim df-info
 RP address: 1.1.1.1
  Interface           State   DF-Pref    DF-Metric  DF-Uptime DF-Address
  GE2/1/1             Win     100        1          01:24:09  192.168.2.1 (local)
  GE2/1/2             Win     100        1          01:24:09  10.110.1.2 (local)
  GE2/1/3             Lose    0          0          01:23:12  10.110.2.2
```

显示 Router C 上双向 PIM 的 DF 信息。

```
[RouterC] display pim df-info
 RP address: 1.1.1.1
  Interface           State   DF-Pref    DF-Metric  DF-Uptime DF-Address
  Loop0               -       -          -          -         -
  GE2/1/1             Win     0          0          01:06:07  10.110.2.2 (local)
  GE2/1/2             Win     0          0          01:06:07  10.110.3.1 (local)
```

显示 Router D 上双向 PIM 的 DF 信息。

```
[RouterD] display pim df-info
 RP address: 1.1.1.1
  Interface           State   DF-Pref    DF-Metric  DF-Uptime DF-Address
  GE2/1/1             Win     100        1          01:19:53  192.168.3.1 (local)
  GE2/1/2             Win     100        1          00:39:34  192.168.4.1 (local)
  GE2/1/3             Lose    0          0          01:21:40  10.110.3.1
```

通过使用 **display multicast forwarding df-info** 命令可以查看路由器上组播转发的 DF 信息，有关 **display multicast forwarding df-info** 命令的详细介绍，请参见“IP 组播命令参考”中的“组播路由与转发”。例如：

显示 Router A 上组播转发的 DF 信息。

```
[RouterA] display multicast forwarding df-info
Total 1 RP, 1 matched

00001. RP address: 1.1.1.1
```

```
    Flags: 0x0
    Uptime: 00:08:32
    RPF interface: GigabitEthernet2/1/2
    List of 1 DF interfaces:
      1: GigabitEthernet2/1/1
```

显示 Router B 上组播转发的 DF 信息。

```
[RouterB] display multicast forwarding df-info
Total 1 RP, 1 matched

00001. RP address: 1.1.1.1
    Flags: 0x0
    Uptime: 00:06:24
    RPF interface: GigabitEthernet2/1/3
    List of 2 DF interfaces:
      1: GigabitEthernet2/1/1
      2: GigabitEthernet2/1/2
```

显示 Router C 上组播转发的 DF 信息。

```
[RouterC] display multicast forwarding df-info
Total 1 RP, 1 matched

00001. RP address: 1.1.1.1
    Flags: 0x0
    Uptime: 00:07:21
    RPF interface: LoopBack0
    List of 2 DF interfaces:
      1: GigabitEthernet2/1/1
      2: GigabitEthernet2/1/2
```

显示 Router D 上组播转发的 DF 信息。

```
[RouterD] display multicast forwarding df-info
Total 1 RP, 1 matched

00001. RP address: 1.1.1.1
    Flags: 0x0
    Uptime: 00:05:12
    RPF interface: GigabitEthernet2/1/3
    List of 2 DF interfaces:
      1: GigabitEthernet2/1/1
      2: GigabitEthernet2/1/2
```

1.8.5 PIM-SSM典型配置举例

1. 组网需求

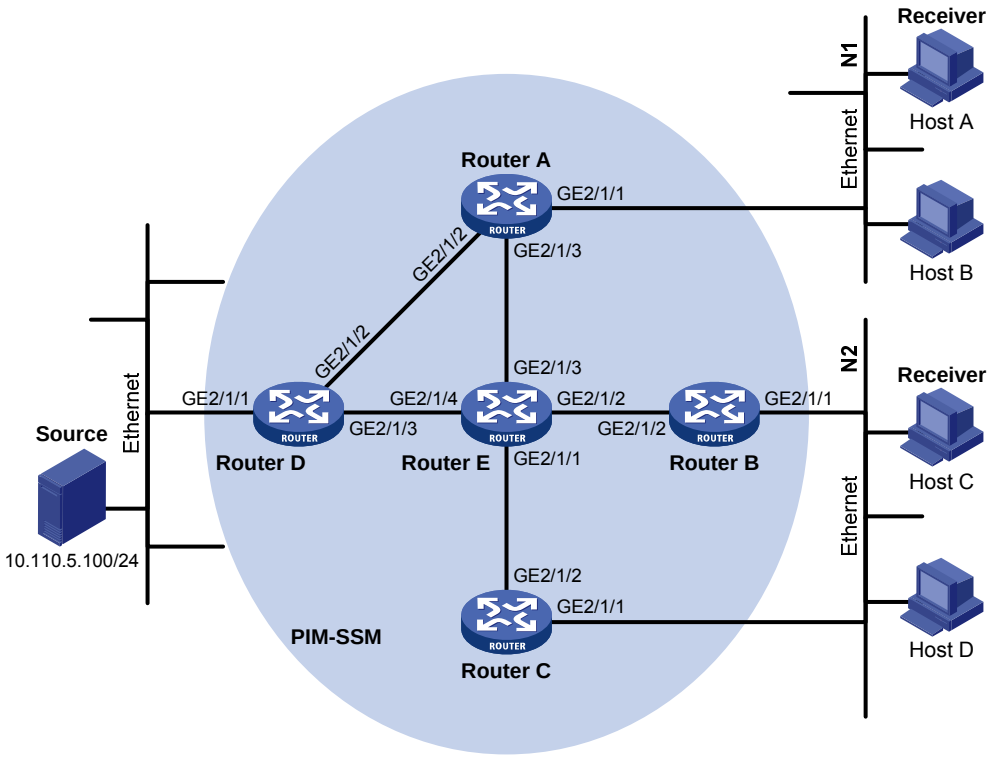
- 接收者通过组播方式接收视频点播信息，不同组织的接收者群体组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 PIM 域采用 SSM 方式。
- Host A 和 Host C 为两个末梢网络中的组播信息接收者；Router D 通过 GigabitEthernet2/1/1 接口与组播源（Source）所在网络连接；Router A 通过 GigabitEthernet2/1/1 接口连接末梢网

络 N1，通过 GigabitEthernet2/1/2 接口和 GigabitEthernet2/1/3 接口分别连接 Router D 和 Router E；Router B 和 Router C 分别通过各自的 GigabitEthernet2/1/1 接口连接末梢网络 N2，并分别通过各自的 GigabitEthernet2/1/2 接口连接 Router E。

- SSM 组播组的范围是 232.1.1.0/24。
- Router A 与末梢网络 N1 之间运行 IGMPv3；Router B 和 Router C 与末梢网络 N2 之间也运行 IGMPv3。

2. 组网图

图1-19 PIM-SSM 典型配置组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	GE2/1/1	10.110.1.1/24	Router D	GE2/1/1	10.110.5.1/24
	GE2/1/2	192.168.1.1/24		GE2/1/2	192.168.1.2/24
	GE2/1/3	192.168.9.1/24		GE2/1/3	192.168.4.2/24
Router B	GE2/1/1	10.110.2.1/24	Router E	GE2/1/1	192.168.3.2/24
	GE2/1/2	192.168.2.1/24		GE2/1/2	192.168.2.2/24
Router C	GE2/1/1	10.110.2.2/24		GE2/1/3	192.168.9.2/24
	GE2/1/2	192.168.3.1/24		GE2/1/4	192.168.4.1/24

3. 配置步骤

(1) 配置 IP 地址和单播路由协议

请按照 图 1-19 配置各接口的IP地址和子网掩码，具体配置过程略。

配置 PIM-SSM 域内的各路由器之间采用 OSPF 协议进行互连，确保 PIM-SSM 域内部在网络层互通，并且各路由器之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，并使能 PIM-SM 和 IGMP

在 Router A 上使能 IP 组播路由，在其连接末梢网络的接口 GigabitEthernet2/1/1 上使能 IGMP，且配置其版本为 3；并在其它接口上使能 PIM-SM。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] igmp enable
[RouterA-GigabitEthernet2/1/1] igmp version 3
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] pim sm
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] interface gigabitethernet 2/1/3
[RouterA-GigabitEthernet2/1/3] pim sm
[RouterA-GigabitEthernet2/1/3] quit
```

Router B 和 Router C 的配置与 Router A 相似，Router D 和 Router E 除了不需要在相应接口上使能 IGMP 外，其它的配置也与 Router A 相似，配置过程略。

(3) 配置 SSM 组播组的地址范围

在 Router A 上配置 SSM 组播组地址范围为 232.1.1.0/24。

```
[RouterA] acl number 2000
[RouterA-acl-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[RouterA-acl-basic-2000] quit
[RouterA] pim
[RouterA-pim] ssm-policy 2000
[RouterA-pim] quit
```

Router B、Router C、Router D 和 Router E 的配置与 Router A 相似，配置过程略。

4. 验证配置

通过使用 **display pim interface** 命令可以查看路由器接口上 PIM 的配置和运行情况。例如：

显示 Router A 上 PIM 的配置信息。

```
[RouterA] display pim interface
 Interface           NbrCnt HelloInt   DR-Pri     DR-Address
 GE2/1/1             0      30         1          10.110.1.1     (local)
 GE2/1/2             1      30         1          192.168.1.2
 GE2/1/3             1      30         1          192.168.9.2
```

假如 Host A 需要接收指定组播源 S（10.110.5.100/24）发往组播组 G（232.1.1.1）的信息，Router A 会向组播源方向构造 SPT，SPT 路径中的路由器（Router A 和 Router D）上生成（S，G）表项，而 SPT 路径之外的路由器（Router E）上没有组播路由项，通过使用 **display pim routing-table** 命令可以查看路由器的 PIM 路由表信息。例如：

显示 Router A 上的 PIM 路由表信息。

```
[RouterA] display pim routing-table
 Total 0 (*, G) entry; 1 (S, G) entry

 (10.110.5.100, 232.1.1.1)
     Protocol: pim-ssm, Flag:
```

```
    UpTime: 00:13:25
    Upstream interface: GigabitEthernet2/1/2
        Upstream neighbor: 192.168.1.2
        RPF prime neighbor: 192.168.1.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/1/1
            Protocol: igmp, UpTime: 00:13:25, Expires: 00:03:25
```

查看 Router D 上的 PIM 路由表信息。

```
[RouterD] display pim routing-table
 Total 0 (*, G) entry; 1 (S, G) entry

 (10.110.5.100, 232.1.1.1)
    Protocol: pim-ssm, Flag: LOC
    UpTime: 00:12:05
    Upstream interface: GigabitEthernet2/1/1
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/1/2
            Protocol:  pim-ssm, UpTime: 00:12:05, Expires: 00:03:25
```

1.9 常见配置错误举例

1.9.1 无法正确建立组播分发树

1. 故障现象

网络中各路由器（包括直连组播源或接收者的路由器）上都没有组播转发项，也就是说无法正确建立组播分发树，客户端无法接收组播数据。

2. 故障分析

- 当全网运行 PIM-DM 时，组播数据由直连组播源的第一跳路由器扩散到直连客户端的最后一跳路由器。无论组播数据扩散到哪一台路由器，只有该路由器存在到达组播源的路由，才会创建（S，G）表项。反之，如果没有到达组播源的路由或者到达组播源的 RPF 接口没有使能 PIM-DM，该路由器就无法创建（S，G）表项。
- 当全网运行 PIM-SM 时，路由器在准备加入 SPT 时，只有存在到达组播源的路由，才会创建（S，G）表项。反之，如果没有到达组播源的路由或者到达组播源的 RPF 接口没有使能 PIM-SM，该路由器就无法创建（S，G）表项。
- 对于某个 RPF 检查对象，在现存的单播路由表中查找到达该对象的最优路由，该路由的出接口作为 RPF 接口，下一跳作为 RPF 邻居。RPF 接口完全依赖于现存的单播路由，并且与 PIM 本身无关。RPF 接口上必须使能 PIM，而且 RPF 邻居也必须是 PIM 邻居。如果 RPF 接口或 RPF 邻居所在路由器上没有使能 PIM，必然使组播分发树无法正确建立，导致组播数据转发异常。

- Hello 报文并不携带 PIM 的模式信息，所以运行 PIM 的路由器无法掌握自己的 PIM 邻居运行的是何种模式的 PIM。如果 RPF 接口和 RPF 邻居所在路由器的对应接口没有使能相同模式的 PIM，必然使组播分发树无法正确建立，导致组播数据转发异常。
- 全网必须运行相同模式的 PIM。否则，组播分发树必然无法正确建立，导致组播数据转发异常。

3. 处理过程

(1) 检查单播路由。使用命令 **display ip routing-table** 命令检查是否有到达组播源或 RP 的单播路由。

(2) 检查接口上是否使能了 PIM，尤其是 RPF 接口上是否使能了 PIM。通过命令 **display pim interface** 命令查看接口上的 PIM 信息。若接口上未使能 PIM，请使用 **pim dm** 或 **pim sm** 命令使能 PIM-DM 或 PIM-SM。

(3) 检查 RPF 邻居是否是 PIM 邻居。通过 **display pim neighbor** 命令查看 PIM 邻居的信息。

(4) 检查直连组播源或接收者的路由器接口上是否使能了 PIM 和 IGMP。

(5) 检查 PIM 模式是否一致。通过命令 **display pim interface verbose** 检查 RPF 接口和 RPF 邻居所在路由器的对应接口上是否使能了相同模式的 PIM。

(6) 检查全网各路由器上的 PIM 模式是否一致。通过命令 **display current-configuration** 查看接口上的 PIM 模式信息，确保全网所有路由器配置有相同模式的 PIM。如果都配置为 PIM-SM，则还需检查 BSR 以及 C-RP 的配置是否正确。

1.9.2 组播数据异常终止在中间路由器

1. 故障现象

组播数据可以到达中间路由器，但无法到达最后一跳路由器。中间路由器某接口上收到组播数据，但 PIM 路由表中没有创建相应的（S，G）表项。

2. 故障分析

- 命令 **multicast boundary** 用于在接口上设置组播转发边界，如果组播数据无法通过该边界，PIM 将无法创建路由项。
- 此外，**source-policy** 命令用于过滤接收到的组播数据报文。如果组播数据报文无法通过该命令中的 ACL 规则，PIM 也无法创建路由项。

3. 处理过程

(1) 检查组播转发边界的配置。通过命令 **display current-configuration** 查看组播转发边界上的设置，使用 **multicast boundary** 命令更改组播转发边界的设置，使组播数据能够通过该边界。

(2) 检查组播过滤器配置。通过命令 **display current-configuration** 查看组播过滤器的配置，更改 **source-policy** 命令的 ACL 规则，使组播数据的源/组地址通过 ACL 过滤。

1.9.3 PIM-SM中RP无法加入SPT

1. 故障现象

RPT 无法正确建立，或者 RP 无法加入到达组播源的 SPT。

2. 故障分析

- RP 是 PIM-SM 网络的核心，为特定的组播组服务，网络中可以同时存在多个 RP。必须保证所有路由器上的 RP 信息完全一致，并且相同的组播组映射到相同的 RP，否则将导致组播数据转发异常。
- 如果使用了静态 RP，必须在全网所有路由器上配置完全相同的静态 RP，否则将导致组播数据转发异常。

3. 处理过程

(1) 检查是否有到达 RP 的单播路由。通过命令 **display ip routing-table** 查看各路由器上是否有到达 RP 的单播路由。

(2) 检查动态 RP 的信息。通过命令 **display pim rp-info** 查看各路由器上的 RP 信息是否一致。

(3) 检查静态 RP 的配置。通过命令 **display pim rp-info** 查看全网所有路由器上的静态 RP 配置是否完全相同。

1.9.4 PIM-SM中无法建立RPT或无法进行源注册

1. 故障现象

C-RP 无法向 BSR 单播通告报文，BSR 没有发布包含 C-RP 的自举报文，BSR 上没有到达各 C-RP 的单播路由，RPT 无法正确建立，或者 DR 无法向 RP 进行源注册。

2. 故障分析

- C-RP 周期性地向 BSR 单播宣告报文，如果 C-RP 没有到达 BSR 的单播路由就无法发送宣告报文，BSR 就收不到 C-RP 宣告报文，也就不会发布包含该 C-RP 的自举报文。
- 另外，如果 BSR 没有到达 C-RP 的单播路由，就会丢弃 C-RP 发来的宣告报文，也不会发布包含该 C-RP 的自举报文。
- RP 是 PIM-SM 网络的核心。必须保证全网所有路由器的 RP 信息完全一致，并且特定的组 G 映射到相同的 RP，以及存在到达 RP 的单播路由。

3. 处理过程

(1) 检查是否有到各 C-RP、BSR 的单播路由。通过命令 **display ip routing-table** 查看各路由器上是否有到达 C-RP 和 BSR 的路由，以及 C-RP 和 BSR 之间的路由是否可达。确保各 C-RP 上存在到达 BSR 的路由，BSR 上存在到达各 C-RP 的路由，全网所有路由器上存在到达 C-RP 的路由。

(2) 检查 RP 和 BSR 信息。PIM-SM 协议需要有 RP 和 BSR 的支持，首先使用命令 **display pim bsr-info** 查看各路由器上是否有 BSR 的信息，使用 **display pim rp-info** 命令查看各路由器上的 RP 信息是否正确。

(3) 检查 PIM 邻居关系。通过命令 **display pim neighbor** 查看各路由器之间是否正确建立了邻居关系。

目 录

1 MSDP


说明

本文中所提到的 DR（Designated Router，指定路由器）、BSR（Bootstrap Router，自举路由器）、C-BSR（Candidate-BSR，候选 BSR）、RP（Rendezvous Point，汇集点）、C-RP（Candidate-RP，候选 RP）、SPT（Shortest Path Tree，最短路径树）和 RPT（Rendezvous Point Tree，共享树）等概念的详细介绍，请参见“IP 组播配置指导”中的“PIM”。

1.1 MSDP简介

MSDP（Multicast Source Discovery Protocol，组播源发现协议）是为了解决多个 PIM-SM（Protocol Independent Multicast Sparse Mode，协议无关组播—稀疏模式）域之间的互连而开发的一种域间组播解决方案，用来发现其它 PIM-SM 域内的组播源信息。

在基本的 PIM-SM 模式下，组播源只向本 PIM-SM 域内的 RP 注册，且各域的组播源信息是相互隔离的，因此 RP 仅知道本域内的组播源信息，只能在本域内建立组播分发树，将本域内组播源发出的组播数据分发给本地用户。如果能够有一种机制，将其它域内的组播源信息传递给本域内的 RP，则本域内的 RP 就可以向其它域内的组播源发起加入过程并建立组播分发树，从而实现组播数据的跨域传输。

基于这一设想，MSDP 通过在网络中选取适当的路由器建立 MSDP 对等体关系，以连通各 PIM-SM 域的 RP。通过在各 MSDP 对等体之间交互 SA（Source Active，信源有效）报文来共享组播源信息。


提示

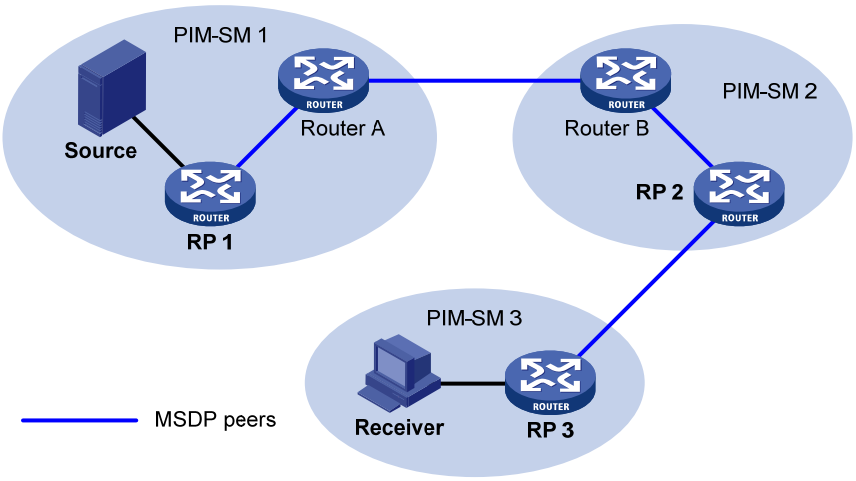
- MSDP 的适用前提：域内组播路由协议必须是 PIM-SM。
- MSDP 仅对 ASM（Any-Source Multicast，任意信源组播）模型有意义。

1.1.1 MSDP原理

1. MSDP对等体

通过在网络中配置一对或多对 MSDP 对等体，形成彼此相连的一张“MSDP 连通图”，以连通各个 PIM-SM 域的 RP。通过这些 MSDP 对等体之间的接力，可以把某 RP 发出的 SA 报文传递给其它所有的 RP。

图1-1 MSDP 对等体的位置



如 图 1-1 所示，MSDP对等体可以创建在任意的PIM-SM路由器上，在不同角色的PIM-SM路由器上所创建的MSDP对等体的功能有所不同：

(1) 在 RP 上创建的 MSDP 对等体

- 源端 MSDP 对等体：即离组播源（Source）最近的 MSDP 对等体（通常也就是源端 RP，如 RP 1）。源端 RP 创建 SA 报文并发送给远端 MSDP 对等体，通告在本 RP 上注册的组播源信息。源端 MSDP 对等体必须配置在 RP 上，否则将无法向外发布组播源信息。
- 接收者端 MSDP 对等体：即离接收者（Receiver）最近的 MSDP 对等体（如 RP 3）。接收者端 MSDP 对等体在收到 SA 报文后，根据该报文中所包含的组播源信息，跨域加入以该组播源为根的 SPT；当来自该组播源的组播数据到达后，再沿 RPT 向本地接收者转发。
- 中间 MSDP 对等体：即拥有多个远端 MSDP 对等体的 MSDP 对等体（如 RP 2）。中间 MSDP 对等体把从一个远端 MSDP 对等体收到的 SA 报文转发给其它远端 MSDP 对等体，其作用相当于传输组播源信息的中转站。

(2) 在普通的 PIM-SM 路由器（非 RP）上创建的 MSDP 对等体

如 Router A 和 Router B，其作用仅限于将收到的 SA 报文转发出去。

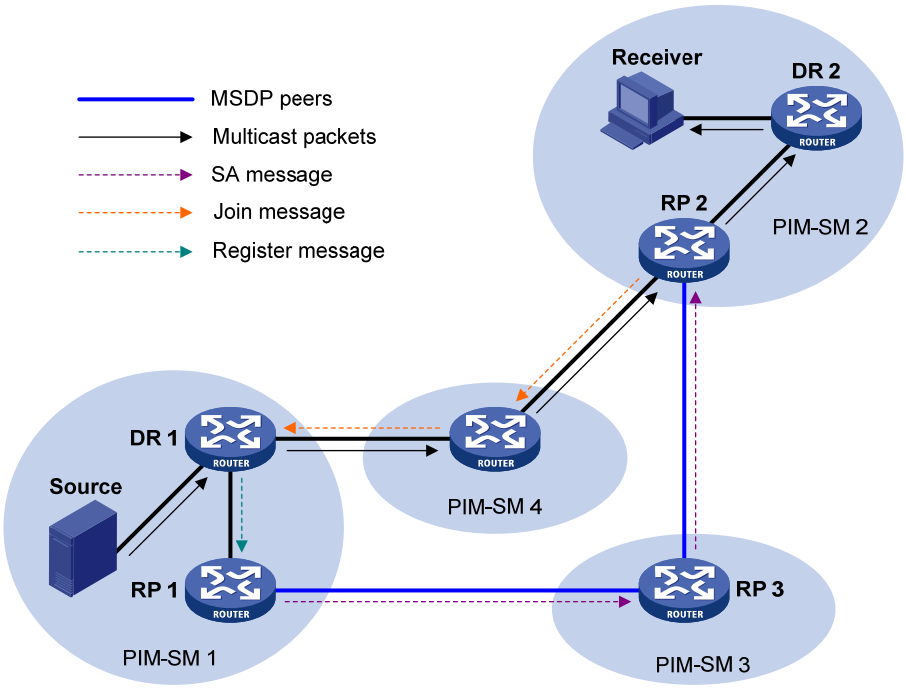
说明

对于通过 BSR 机制动态选举 RP 的 PIM-SM 网络来说，RP 是由 C-RP 选举产生的。为了增强其网络的健壮性，一个 PIM-SM 域内往往存在不止一个 C-RP。由于无法预计 RP 选举的结果，为了保证选举获胜的 C-RP 能始终位于“MSDP 连通图”上，需要在所有的 C-RP 之间建立 MSDP 对等体关系。而选举落败的 C-RP 在“MSDP 连通图”上所担当的角色相当于普通的 PIM-SM 路由器。

2. MSDP实现域间组播

如 图 1-2 所示，PIM-SM 1 域内存在激活的组播源（Source），RP 1 通过组播源注册过程了解到了该组播源的存在。如果PIM-SM 2 和PIM-SM 3 域也希望知道该组播源的具体位置，进而能够从该组播源获取组播数据，则需要在RP 1 与RP 3、RP 2 与RP 3 之间分别建立MSDP对等体关系。

图1-2 MSDP 实现域间组播示意图



借助 MSDP 对等体进行 PIM-SM 域间组播的工作过程如下：

(1) 当 PIM-SM 1 域内的组播源向组播组 G 发送第一个组播数据包时，DR 1 将该组播数据封装在注册报文（Register Message）中，并发给 RP 1。RP 1 因此获知了该组播源的相关信息。

(2) RP 1 作为源端 RP，创建 SA 报文，并周期性地向其它 MSDP 对等体发送。SA 报文中包含组播源的地址 S、组播组的地址 G 以及创建该 SA 报文的源端 RP（即 RP 1）的地址。

(3) MSDP 对等体对收到的 SA 报文进行 RPF（Reverse Path Forwarding，逆向路径转发）检查，以及各种转发策略的过滤，从而只接受和转发来自正确路径并通过过滤的 SA 报文，以避免 SA 报文传递环路；另外，可以在 MSDP 对等体之间配置 MSDP 全连接组（Mesh Group），以避免 SA 报文在 MSDP 对等体之间的泛滥。

(4) SA 报文在 MSDP 对等体之间转发，最终该组播源的相关信息将传遍所有建立了 MSDP 对等体关系的 PIM-SM 域（即 PIM-SM 2 和 PIM-SM 3）。

(5) PIM-SM 2 中的 RP 2 在收到该 SA 报文后，检查本域内是否有组播组 G 的接收者（Receiver）存在：

- 如果有接收者，RP 2 与接收者之间维护组播组 G 的 RPT。RP 2 创建（S，G）表项，向组播源方向逐跳发送（S，G）加入报文（Join Message），从而跨越各 PIM-SM 域在沿途形成 SPT。组播数据沿 SPT 到达 RP 2 后，再沿 RPT 向接收者转发。当接收者侧的 DR 2 收到来自组播源的组播数据后，可根据配置来决定是否发起 SPT 切换；
- 如果没有接收者，RP 2 不会创建（S，G）表项，也不会向组播源方向发送加入报文。

说明

- MSDP 全连接组：要求所有组成员之间两两建立 MSDP 对等体关系，且所有组成员均使用相同的组名称。
- 在使用 MSDP 进行域间组播时，RP 在收到组播源的信息后就不再需要依赖其它 PIM-SM 域内的 RP，此时接收者可以跨越各 PIM-SM 域内的 RP，而直接加入基于组播源的 SPT。

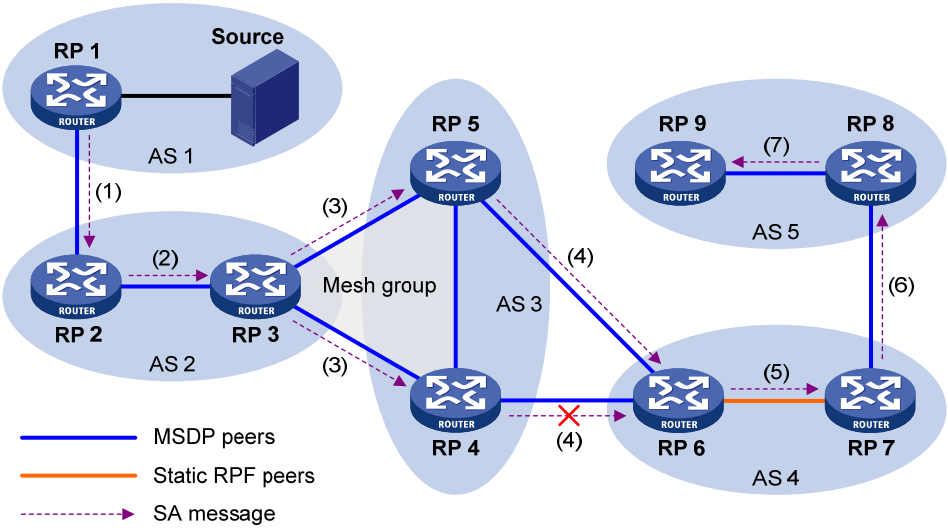
3. SA报文的RPF检查规则

如 图 1-3 所示，网络中有五个自治系统AS 1～AS 5，AS内部使用IGP互联，AS之间使用BGP或MBGP互联。每个AS中包含至少一个PIM-SM域，且每个PIM-SM域中包含至少一个RP。各RP之间建立起MSDP对等体关系，其中RP 3、RP 4 和RP 5 之间建立MSDP全连接组，并在RP 7 上将RP 6 配置为其静态RPF对等体。

说明

设备对于来自静态 RPF 对等体的 SA 报文不进行 RPF 检查，直接接受并向其它对等体转发。

图1-3 SA 报文的 RPF 检查规则



对照 图 1-3，这些MSDP对等体将按照如下RPF检查规则处理收到的SA报文：

(1) 当 RP 2 收到 RP 1 发来的 SA 报文时：由于 SA 报文中所携带的源端 RP 的地址与 MSDP 对等体的地址相同，说明发出 SA 报文的 MSDP 对等体就是创建该 SA 报文的 RP，于是 RP 2 接受该 SA 报文并向其它对等体（RP 3）转发。

(2) 当 RP 3 收到 RP 2 发来的 SA 报文时：由于 SA 报文来自同一个 AS 的 MSDP 对等体（RP 2），且该对等体是到源端 RP 最佳路径上的下一跳，于是 RP 3 接受该 SA 报文并向其它对等体（RP 4 和 RP 5）转发。

(3) 当 RP 4 和 RP 5 分别收到 RP 3 发来的 SA 报文时：由于 SA 报文来自同一个全连接组的 MSDP 对等体（RP 3），于是 RP 4 和 RP 5 均接受该 SA 报文并不再向本组其它成员转发，而只向本组之外的其它 MSDP 对等体（RP 6）转发。

(4) 当 RP 6 收到 RP 4 和 RP 5（假设 RP 5 的 IP 地址较大）发来的 SA 报文时：尽管同处 AS 3 的 RP 4 和 RP 5 都与 RP 6 建立了 MSDP 对等体关系，但 RP 6 只接受 IP 地址较高的 MSDP 对等体（RP 5）发来的 SA 报文。

(5) 当 RP 7 收到 RP 6 发来的 SA 报文时：由于 SA 报文来自其静态 RPF 对等体（RP 6），于是 RP 7 接受该 SA 报文并向其它对等体（RP 8）转发。

(6) 当 RP 8 收到 RP 7 发来的 SA 报文时：属于不同 AS 的 MSDP 对等体之间存在 BGP 或 MBGP 路由。由于 SA 报文来自不同 AS 的 MSDP 对等体（RP 7），且该对等体是到源端 RP 的 BGP 或 MBGP 路由的下一跳，于是 RP 8 接受该 SA 报文并向其它对等体（RP 9）转发。

(7) 当 RP 9 收到 RP 8 发来的 SA 报文时：由于只有一个 MSDP 对等体（RP 8），于是 RP 9 接受该 SA 报文。

对于由其它路径到来的 SA 报文，MSDP 对等体将不接受也不转发。

4. 基于MSDP实现Anycast-RP

PIM-SM 要求每个组播组只能有一个激活的 RP，因此当某 RP 失效时，可能导致其对应组播组的流量中断。Anycast-RP 机制通过为同一组播组设置具有相同地址的多个 RP，组播源和接收者各自就近选择 RP 进行注册或加入，这些 RP 之间则进行组播源信息的同步，从而实现了 RP 间的冗余备份。Anycast-RP 具有以下优点：

- RP 路径最优：组播源向距离最近的 RP 进行注册，建立路径最优的 SPT；接收者向距离最近的 RP 发起加入，建立路径最优的 RPT。
- RP 冗余备份：当某 RP 失效后，原先在该 RP 上注册或加入的组播源或接收者会自动选择就近的 RP 进行注册或加入，从而实现了 RP 间的冗余备份。

Anycast-RP 可以通过以下两种方式实现：

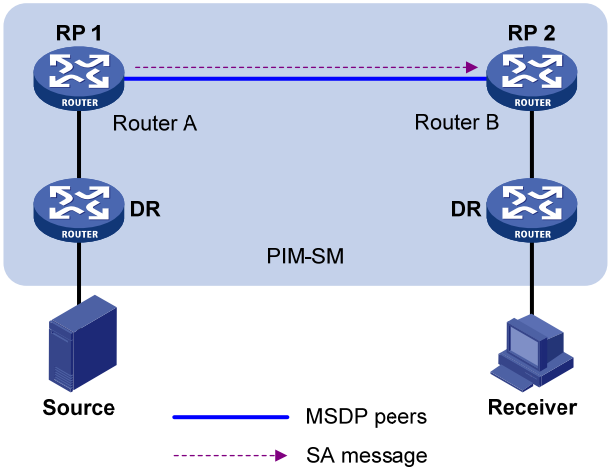
- 基于 PIM-SM 实现：通过对 RP 进行一定的扩展来实现，不需要依赖 MSDP。详细介绍请参见“IP 组播配置指导”中的“PIM”。
- 基于 MSDP 实现：通过为同一组播组设置具有相同地址的多个 RP，并在这些 RP 之间建立 MSDP 对等体关系来实现。本文主要介绍这种实现方式。

基于MSDP的实现如 图 1-4 所示。在一个PIM-SM域内，组播源（Source）向组播组G发送组播数据，接收者（Receiver）是组播组G的成员。分别在Router A和Router B上配置相同的IP地址（即Anycast-RP地址，通常使用私有地址），将这些接口配置为C-RP，并在Router A和Router B之间建立MSDP对等体关系。

提示

- 通常在设备的逻辑接口（如 LoopBack 接口）上配置 Anycast-RP 地址。
- 充当 Anycast-RP 的接口地址必须为主机地址（即子网掩码为 255.255.255.255）。
- MSDP 对等体的地址不能与 Anycast-RP 地址相同。

图1-4 基于 MSDP 实现 Anycast-RP 示意图



基于 MSDP 实现 Anycast-RP 的工作过程如下：

(1) 当组播源测 DR 收到来自组播源的组播数据时，选择距离最近的 RP（本例中为 RP 1）进行注册。

(2) 当接收者侧 DR 收到接收者的加入请求时，向距离最近的 RP（本例中为 RP 2）发送加入报文，从而形成以该 RP 为根的 RPT。

(3) 各 RP 之间通过交互 SA 报文，共享组播源信息。当 RP 2 获得组播源信息后，向组播源方向发送加入报文，从而在沿途形成 SPT。

(4) 当组播数据沿 SPT 到达 RP 2 后，再沿 RPT 向接收者转发；接收者侧 DR 收到组播数据后，可根据配置来决定是否发起 SPT 切换。

1.1.2 多实例的MSDP

属于同一实例的组播路由器各接口之间可以建立 MSDP 对等体。通过在 MSDP 对等体之间交互 SA 报文，可以实现跨域的 VPN 组播。

应用多实例的组播路由器，为其所支持的每一个实例都独立维护了一套 MSDP 机制，包括：SA 缓存、对等体连接、定时器、发送缓存和 PIM 交互的缓冲区。同时，保证不同实例之间信息隔离。所以，只有属于同一实例的 MSDP 和 PIM-SM 信息才可以交互。

1.1.3 协议规范

与 MSDP 相关的协议规范有：

- RFC 3618：Multicast Source Discovery Protocol (MSDP)
- RFC 3446：Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)

1.2 MSDP配置任务简介

表1-1 MSDP 配置任务简介

配置任务		说明	详细配置
配置MSDP基本功能	使能MSDP	必选	1.3.2
	创建MSDP对等体连接	必选	1.3.3
	配置静态RPF对等体	可选	1.3.4
配置MSDP对等体连接	配置MSDP对等体描述信息	可选	1.4.2
	配置MSDP全连接组	可选	1.4.3
	配置MSDP对等体连接控制	可选	1.4.4
配置SA报文	配置SA报文内容	可选	1.5.2
	配置SA请求报文	可选	1.5.3
	配置SA报文过滤规则	可选	1.5.4
	配置SA报文缓存	可选	1.5.5

1.3 配置MSDP基本功能

说明

本节的所有配置都是在 PIM-SM 域内的 RP 上进行的，这些 RP 将成为 MSDP 对等体的一端。

1.3.1 配置准备

在配置 MSDP 基本功能之前，需完成以下任务：

- 配置任一单播路由协议，实现域内网络层互通
- 配置 PIM-SM，实现域内组播

1.3.2 使能MSDP

在配置 MSDP 各功能之前，必须先使能 MSDP。

表1-2 使能 MSDP

操作	命令	说明
进入系统视图	**system-view**	-
使能IP组播路由，并进入MRIB视图	**multicast routing** [**vpn-instance** *vpn-instance-name*]	缺省情况下，IP组播路由处于关闭状态 本命令的详细介绍请参见“IP组播命令参考”中的“组播路由与转发”

操作	命令	说明
退回系统视图	**quit**	-
使能MSDP，并进入MSDP视图	**msdp** [**vpn-instance** *vpn-instance-name*]	MSDP处于关闭状态

1.3.3 创建MSDP对等体连接

MSDP 对等体使用地址对来标识，即本端 MSDP 对等体地址和远端 MSDP 对等体地址。需要在互为对等体的两端都创建 MSDP 对等体连接。

说明

如果某接口同时作为 MSDP 对等体和 BGP/MBGP 对等体中的一端，则建议为 MSDP 对等体配置与 BGP 或 MBGP 对等体相同的 IP 地址。

表1-3 创建 MSDP 对等体连接

操作	命令	说明
进入系统视图	**system-view**	-
进入MSDP视图	**msdp** [**vpn-instance** *vpn-instance-name*]	-
创建MSDP对等体连接	**peer** *peer-address* **connect-interface** *interface-type interface-number*	缺省情况下，没有创建MSDP对等体连接

1.3.4 配置静态RPF对等体

通过配置静态 RPF 对等体可以免除对收到的 SA 报文进行 RPF 检查。

说明

如果在一台路由器上只配置了一个 MSDP 对等体，则该 MSDP 对等体将被当作静态 RPF 对等体。

表1-4 配置静态 RPF 对等体

操作	命令	说明
进入系统视图	**system-view**	-
进入MSDP视图	**msdp** [**vpn-instance** *vpn-instance-name*]	-
配置静态RPF对等体	**static-rpf-peer** *peer-address* [**rp-policy** *ip-prefix-name*]	缺省情况下，不存在任何静态RPF对等体

1.4 配置MSDP对等体连接

1.4.1 配置准备

在配置 MSDP 对等体连接之前，需完成以下任务：

- 配置任一单播路由协议，实现域内网络层互通
- 配置 MSDP 基本功能

1.4.2 配置MSDP对等体描述信息

管理员可以通过MSDP对等体的描述信息方便地区分不同的MSDP对等体，从而更好地管理MSDP对等体。

表1-5 配置 MSDP 对等体描述信息

操作	命令	说明
进入系统视图	**system-view**	-
进入MSDP视图	**msdp** [**vpn-instance** *vpn-instance-name*]	-
配置MSDP对等体的描述信息	**peer** *peer-address* **description** *text*	缺省情况下，MSDP对等体没有描述信息

1.4.3 配置MSDP全连接组

一个自治系统内可能包含多个 MSDP 对等体，为了避免这些 MSDP 对等体之间泛滥 SA 报文，可以使用 MSDP 全连接组来优化数据流量。

构成全连接组的 MSDP 对等体，一方面将来自组外并通过了 RPF 检查的 SA 报文转发给组内的其它成员；另一方面，对来自组内成员的 SA 报文不经 RPF 检查就接受，也不在组内进行重复转发。这种操作既避免了 SA 报文的泛滥，同时还由于不需要在 MSDP 对等体之间运行 BGP 或 MBGP，所以也就简化了对等体 RPF 检查机制。

通过为多个 MSDP 对等体配置相同的全连接组名称，可以建立 MSDP 全连接组。

说明

- 在配置 MSDP 全连接组之前，应使各路由器之间保持两两互连。
- 如果在同一 MSDP 对等体上多次配置加入全连接组，最后一个配置有效。

表1-6 配置 MSDP 全连接组

操作	命令	说明
进入系统视图	**system-view**	-
进入MSDP视图	**msdp** [**vpn-instance** *vpn-instance-name*]	-

操作	命令	说明
把MSDP对等体加入全连接组	**peer** *peer-address* **mesh-group** *name*	缺省情况下，MSDP对等体不属于任何全连接组

1.4.4 配置MSDP对等体连接控制

MSDP 对等体之间使用 TCP 进行连接（端口号为 639），用户可以手工关闭或重建 MSDP 对等体连接，灵活控制 MSDP 对等体之间的会话。当关闭了 MSDP 对等体连接后，MSDP 对等体之间不再传递 SA 报文，TCP 连接关闭，并不再重试建立连接，但配置信息会被保留。

当 MSDP 对等体之间建立会话后，会定时互发 Keepalive 报文（其发送间隔被称为保活时间），以免对端认为会话已中断。如果一端在保持时间内未收到对端的 Keepalive 报文或其它报文，便断开此会话。由于 MSDP 对等体之间没有保活时间和保持时间的协商机制，因此必须为两端配置相同的保活时间和保持时间，且保活时间必须小于保持时间。

当新创建了 MSDP 对等体、或重新启动了被关闭的 MSDP 对等体连接、或发生故障的 MSDP 对等体尝试恢复工作时，需要在 MSDP 对等体之间建立 TCP 连接。用户可以灵活地调整建立 MSDP 对等体连接的重试周期。

为了提高 MSDP 的安全性，可以配置 MSDP 对等体在建立 TCP 连接时进行 MD5 认证。该认证并不能对 MSDP 报文进行认证，它只是为 TCP 连接设置 MD5 认证密钥，并由 TCP 完成认证。如果认证失败，则无法建立 TCP 连接。

提示

参与 MD5 认证的两端 MSDP 对等体必须配置相同的认证方式和密钥，否则将由于不能通过认证而无法建立 TCP 连接。

表1-7 配置 MSDP 对等体连接控制

操作	命令	说明
进入系统视图	**system-view**	-
进入MSDP视图	**msdp** [**vpn-instance** *vpn-instance-name*]	-
关闭MSDP对等体连接	**shutdown** *peer-address*	缺省情况下，MSDP对等体的连接处于开启状态
配置MSDP对等体会话的保活时间和保持时间	**timer keepalive** *keepalive holdtime*	缺省情况下，MSDP会话的保活时间为60秒，保持时间为75秒 本命令会对已建立的MSDP会话立即生效
配置建立MSDP对等体连接的重试周期	**timer retry** *interval*	缺省情况下，建立MSDP对等体连接的重试周期为30秒
配置MSDP对等体建立TCP连接时进行MD5认证	**peer** *peer-address* **password** { **cipher** | **simple** } *password*	缺省情况下，MSDP对等体建立TCP连接时不进行MD5认证

1.5 配置SA报文

1.5.1 配置准备

在配置 SA 报文传递之前，需完成以下任务：

- 配置任一单播路由协议，实现域内网络层互通
- 配置 MSDP 基本功能

1.5.2 配置SA报文内容

某些组播源发送组播数据的时间间隔较长，超出了（S，G）表项的超时时间。在这种情况下，源端 DR 只能将组播数据逐个封装在注册报文中，发送给源端 RP。源端 RP 使用 SA 报文将（S，G）信息传输给远端 RP。然后，远端 RP 向源端 DR 发起加入过程，并创建 SPT。由于（S，G）表项已超时，远端用户将永远无法收到该组播源发出的组播数据。

当在源端 RP 上使能了在 SA 报文中封装组播数据报文的功能后，源端 RP 会将组播数据报文封装在 SA 报文中发送出去。远端 RP 收到该 SA 报文后解封装，并将组播数据报文沿 RPT 传输给本域内的用户。

MSDP 对等体之间传递 SA 报文，当路由器对收到的 SA 报文进行 RPF 检查时，如果发现对端 RP 的地址与本地 RP 的地址相同，就会丢弃该 SA 报文。但在 Anycast-RP 应用中，要求在同一个 PIM-SM 域内的两台或多台路由器上配置 IP 地址相同的 RP，并在这些路由器之间建立 MSDP 对等体关系，因此必须为 SA 报文指定一个与实际 RP 的地址不同的逻辑 RP 地址（即逻辑接口上的 RP 地址），以通过 RPF 检查。

表1-8 配置 SA 报文内容

操作	命令	说明
进入系统视图	**system-view**	-
进入MSDP视图	**msdp** [**vpn-instance** *vpn-instance-name*]	-
使能在SA报文中封装组播数据报文	**encap-data-enable**	缺省情况下，在SA报文中只包含（S，G）表项，不封装组播数据报文
将接口地址配置为SA报文的RP地址	**originating-rp** *interface-type interface-number*	缺省情况下，SA报文的RP地址为PIM的RP地址

1.5.3 配置SA请求报文

缺省情况下，当一个新接收者加入时，路由器不会主动向其 MSDP 对等体发送 SA 请求报文，而是等待其 MSDP 对等体在下一个周期发来的 SA 报文，这将延迟接收者获取组播源信息的时间。为了尽快让新接收者了解到当前活跃的组播源信息，需要主动向 MSDP 对等体发送 SA 请求报文。

提示

在使能发送 SA 请求报文功能之前，必须首先关闭 SA 报文缓存机制，否则设备不会向外发送 SA 请求报文。

表1-9 配置 SA 请求报文

操作	命令	说明
进入系统视图	**system-view**	-
进入MSDP视图	**msdp** [**vpn-instance** *vpn-instance-name*]	-
使能发送SA请求报文	**peer** *peer-address* **request-sa-enable**	缺省情况下，路由器收到新的组加入报文时，不向其MSDP对等体发送SA请求报文，而是等待下一周期SA报文的到来
配置SA请求报文的过滤规则	**peer** *peer-address* **sa-request-policy** [**acl** *acl-number*]	缺省情况下，不对SA请求报文进行过滤

1.5.4 配置SA报文过滤规则

通过配置 SA 报文的创建规则，路由器可以在创建 SA 报文时，对其通告的（S，G）表项进行过滤，从而实现在创建 SA 报文时对组播源消息传播的控制。

通过配置接收或转发 SA 报文的过滤规则，路由器可以在接收或转发 SA 报文时，对其通告的（S，G）转发项进行过滤，从而实现在接收和转发 SA 报文时，对组播源消息传播的控制。

通过配置封装在 SA 报文中组播数据报文的 TTL 阈值，可以对组播数据报文在 SA 报文中的封装以及传输范围进行限制：

- 路由器在创建封装有组播数据报文的 SA 报文之前，先检查该组播数据报文 IP 头的 TTL 值：如果小于阈值，则不创建该 SA 报文；如果大于或等于阈值，则将组播数据报文封装在 SA 报文中并转发出去。
- 路由器在收到封装有组播数据报文的 SA 报文之后，先将该组播数据报文 IP 头的 TTL 值减 1，再检查此时的 TTL 值：如果小于阈值，则不再向其指定的 MSDP 对等体转发；如果大于或等于阈值，则重新将组播数据报文封装在 SA 报文中并转发出去。

表1-10 配置 SA 报文过滤规则

操作	命令	说明
进入系统视图	**system-view**	-
进入MSDP视图	**msdp** [**vpn-instance** *vpn-instance-name*]	-
配置SA报文的创建规则	**import-source** [**acl** *acl-number*]	缺省情况下，在创建SA报文时，对其通告的（S，G）表项不作限制
配置接收或转发SA报文的过滤规则	**peer** *peer-address* **sa-policy** { **export** | **import** } [**acl** *acl-number*]	缺省情况下，不对接收或转发的SA报文进行过滤

操作	命令	说明
配置封装在SA报文中组播数据报文的最小TTL值	**peer** *peer-address* **minimum-ttl** *ttl-value*	缺省情况下，封装在SA报文中组播数据报文的最小TTL值为0

1.5.5 配置SA报文缓存

为了减少获取组播信息的延迟时间，可以在路由器上使能 SA 报文缓存机制，即在本地缓存 SA 报文中所包含的（S，G）表项。缓存的（S，G）表项越多，所占用的内存空间越大。

在使能了 SA 报文缓存机制后，当收到一个新的组加入报文（*，G）时，路由器首先查找 SA 缓存：

- 如果缓存中没有对应的（S，G），便等候其 MSDP 对等体在下一个周期发来的 SA 报文；
- 如果缓存中有对应的（S，G），则直接加入以 S 为根的 SPT。

为了有效防止路由器受到 DoS（Denial of Service，拒绝服务）攻击，可以在路由器上配置可缓存（S，G）表项的最大数量。

表1-11 配置 SA 报文缓存

操作	命令	说明
进入系统视图	**system-view**	-
进入MSDP视图	**msdp** [**vpn-instance** *vpn-instance-name*]	-
使能SA报文缓存机制	**cache-sa-enable**	在缺省情况下，SA报文缓存机制处于使能状态，即在设备收到SA报文后缓存其中包含的（S，G）表项
配置可缓存从指定MSDP对等体学到的（S，G）表项的最大数量	**peer** *peer-address* **sa-cache-maximum** *sa-limit*	缺省情况下，可缓存从任一MSDP对等体学到的（S，G）表项的最大数量为4294967295

1.6 MSDP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 MSDP 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 MSDP 的统计信息。

表1-12 MSDP 显示和维护

操作	命令
显示MSDP对等体的简要信息	**display msdp** [**vpn-instance** *vpn-instance-name*] **brief** [**state** { **connect** | **disabled** | **established** | **listen** | **shutdown** }]
显示MSDP对等体的详细状态信息	**display msdp** [**vpn-instance** *vpn-instance-name*] **peer-status** [*peer-address*]
显示SA缓存中的（S，G）表项信息	**display msdp** [**vpn-instance** *vpn-instance-name*] **sa-cache** [*group-address* | *source-address* | *as-number*] *
显示SA缓存中（S，G）表项的数量	**display msdp** [**vpn-instance** *vpn-instance-name*] **sa-count** [*as-number*]

操作	命令
重置与MSDP对等体的TCP连接，并清除MSDP对等体的所有统计信息	**reset msdp** [**vpn-instance** *vpn-instance-name*] **peer** [*peer-address*]
清除SA缓存中的（S，G）表项	**reset msdp** [**vpn-instance** *vpn-instance-name*] **sa-cache** [*group-address*]
在不重置MSDP对等体的情况下，清除MSDP对等体的统计信息	**reset msdp** [**vpn-instance** *vpn-instance-name*] **statistics** [*peer-address*]

1.7 MSDP典型配置举例

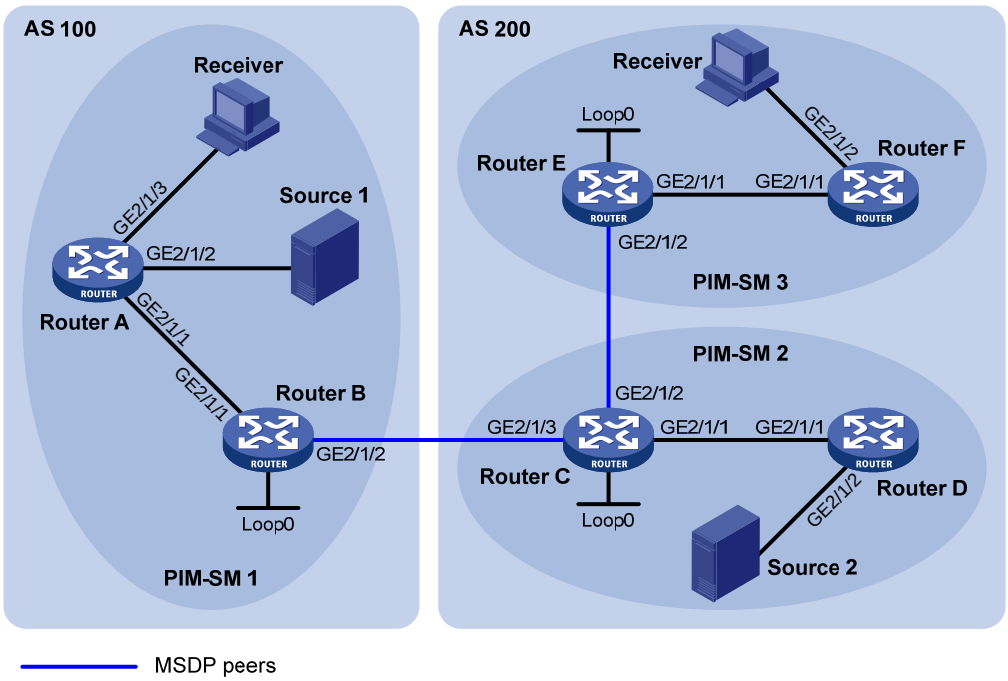
1.7.1 PIM-SM域间组播配置举例

1. 组网需求

- 网络中存在两个自治系统：AS 100 和 AS 200，各 AS 内部采用 OSPF 协议、AS 之间则采用 BGP 协议以保证单播路由的畅通；
- PIM-SM 1 属于 AS 100，PIM-SM 2 和 PIM-SM 3 属于 AS 200，每个 PIM-SM 域分别拥有至少一个组播源（Source）或接收者（Receiver）；
- 将 Router B、Router C 和 Router E 各自的 LoopBack0 接口分别配置为各自 PIM-SM 域的 C-BSR 和 C-RP；
- 通过在各 PIM-SM 域的 RP 之间建立 MSDP 对等体，从而实现各 PIM-SM 域之间组播源信息的共享。

2. 组网图

图1-5 PIM-SM 域间组播配置组网图



设备	接口	IP地址	设备	接口	IP地址

Router A	GE2/1/1	10.110.1.2/24	Router D	GE2/1/1	10.110.4.2/24
	GE2/1/2	10.110.2.1/24		GE2/1/2	10.110.5.1/24
	GE2/1/3	10.110.3.1/24	Router E	GE2/1/1	10.110.6.1/24
Router B	GE2/1/1	10.110.1.1/24		GE2/1/2	192.168.3.2/24
	GE2/1/2	192.168.1.1/24		Loop0	3.3.3.3/32
	Loop0	1.1.1.1/32	Router F	GE2/1/1	10.110.6.2/24
Router C	GE2/1/1	10.110.4.1/24		GE2/1/2	10.110.7.1/24
	GE2/1/2	192.168.3.1/24	Source 1	-	10.110.2.100/24
	GE2/1/3	192.168.1.2/24	Source 2	-	10.110.5.100/24
	Loop0	2.2.2.2/32			

3. 配置步骤

(1) 配置 IP 地址和单播路由协议

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。

配置 AS 内的各路由器之间采用 OSPF 协议进行互连，确保各 AS 内部在网络层互通，并且各路由器之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，使能 PIM-SM 和 IGMP，并配置 BSR 的服务边界

在 Router A 上使能 IP 组播路由，在主机侧接口 GigabitEthernet2/1/3 上使能 IGMP，并在其它接口上使能 PIM-SM。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] pim sm
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] pim sm
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] interface gigabitethernet 2/1/3
[RouterA-GigabitEthernet2/1/3] igmp enable
[RouterA-GigabitEthernet2/1/3] quit
```

Router B、Router C、Router D、Router E 和 Router F 上的配置与 Router A 相似，配置过程略。

在 Router B 上配置 BSR 的服务边界。

```
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] pim bsr-boundary
[RouterB-GigabitEthernet2/1/2] quit
```

Router C 和 Router E 上的配置与 Router B 相似，配置过程略。

(3) 配置 C-BSR 和 C-RP 的位置

在 Router B 上将 LoopBack0 接口配置为 C-BSR 和 C-RP。

```
[RouterB] pim
[RouterB-pim] c-bsr 1.1.1.1
[RouterB-pim] c-rp 1.1.1.1
[RouterB-pim] quit
```

Router C 和 Router E 上的配置与 Router B 相似，配置过程略。

(4) 配置 BGP 协议，将 BGP 与 OSPF 互相引入

在 Router B 上配置 EBGP 对等体，并引入 OSPF 路由。

```
[RouterB] bgp 100
[RouterB-bgp] router-id 1.1.1.1
[RouterB-bgp] peer 192.168.1.2 as-number 200
[RouterB-bgp] address-family ipv4
[RouterB-bgp-ipv4] import-route ospf 1
[RouterB-bgp-ipv4] peer 192.168.1.2 enable
[RouterB-bgp-ipv4] quit
[RouterB-bgp] quit
```

在 Router C 上配置 EBGP 对等体，并引入 OSPF 路由。

```
[RouterC] bgp 200
[RouterC-bgp] router-id 2.2.2.2
[RouterC-bgp] peer 192.168.1.1 as-number 100
[RouterC-bgp] address-family ipv4
[RouterC-bgp-ipv4] import-route ospf 1
[RouterB-bgp-ipv4] peer 192.168.1.1 enable
[RouterC-bgp-ipv4] quit
[RouterC-bgp] quit
```

在 Router B 的 OSPF 中引入 BGP。

```
[RouterB] ospf 1
[RouterB-ospf-1] import-route bgp
[RouterB-ospf-1] quit
```

在 Router C 的 OSPF 中引入 BGP。

```
[RouterC] ospf 1
[RouterC-ospf-1] import-route bgp
[RouterC-ospf-1] quit
```

(5)　配置 MSDP 对等体

在 Router B 上配置 MSDP 对等体。

```
[RouterB] msdp
[RouterB-msdp] peer 192.168.1.2 connect-interface gigabitethernet 2/1/2
[RouterB-msdp] quit
```

在 Router C 上配置 MSDP 对等体。

```
[RouterC] msdp
[RouterC-msdp] peer 192.168.1.1 connect-interface gigabitethernet 2/1/3
[RouterC-msdp] peer 192.168.3.2 connect-interface gigabitethernet 2/1/2
[RouterC-msdp] quit
```

在 Router E 上配置 MSDP 对等体。

```
[RouterE] msdp
[RouterE-msdp] peer 192.168.3.1 connect-interface gigabitethernet 2/1/2
[RouterE-msdp] quit
```

4. 验证配置

通过使用 **display bgp peer ipv4 unicast** 命令可以查看路由器之间 BGP IPv4 单播对等体或对等体组的信息。例如：

显示 Router B 上 BGP IPv4 单播对等体或对等体组的信息。

```
[RouterB] display bgp peer ipv4
```

```
 BGP local router ID: 1.1.1.1
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  192.168.1.2            200       24       21    0       6 00:13:09 Established
```

显示 Router C 上 BGP IPv4 单播对等体或对等体组的信息。

```
[RouterC] display bgp peer ipv4

 BGP local router ID: 2.2.2.2
 Local AS number: 200
 Total number of peers: 1                 Peers in established state: 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  192.168.1.1            100       18       16    0       1 00:12:04 Established
```

通过使用 **display bgp routing-table ipv4 unicast** 命令可以查看路由器上 BGP IPv4 单播路由的信息。例如：

显示 Router C 上 BGP IPv4 单播路由的信息。

```
[RouterC] display bgp routing-table ipv4

Total number of routes: 5

 BGP local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >  1.1.1.1/32         192.168.1.1     0                     0       100?
* >i 2.2.2.2/32         0.0.0.0         0                     0       ?
* >  192.168.1.0        0.0.0.0         0                     0       ?
* >  192.168.1.1/32     0.0.0.0         0                     0       ?
* >  192.168.1.2/32     0.0.0.0         0                     0       ?
```

当 PIM-SM 1 和 PIM-SM 2 域内的组播源 Source 1 和 Source 2 发送组播信息时，PIM-SM 1 和 PIM-SM 3 域内的接收者能收到该组播信息。通过使用 **display msdp brief** 命令可以查看路由器之间 MSDP 对等体的简要信息。例如：

显示 Router B 上 MSDP 对等体的简要信息。

```
[RouterB] display msdp brief
Configured   Established  Listen       Connect      Shutdown     Disabled
1            1            0            0            0            0

Peer address    State       Up/Down time    AS         SA count   Reset count
192.168.1.2     Established 00:12:19        200        13         0
```

显示 Router C 上 MSDP 对等体的简要信息。

```
[RouterC] display msdp brief
Configured   Established  Listen       Connect      Shutdown     Disabled
2            2            0            0            0            0

Peer address    State       Up/Down time    AS         SA count   Reset count
192.168.3.2     Established 00:15:19        200        8          0
192.168.1.1     Established 00:06:11        100        13         0
```

显示 Router E 上 MSDP 对等体的简要信息。

```
[RouterE] display msdp brief
Configured   Established  Listen       Connect      Shutdown     Disabled
1            1            0            0            0            0

Peer address    State       Up/Down time    AS         SA count   Reset count
192.168.3.1     Established 01:12:19        200        8          0
```

显示 Router B 上 MSDP 对等体的详细状态信息。

```
[RouterB] display msdp peer-status
MSDP Peer 192.168.1.2; AS 200
 Description:
 Information about connection status:
   State: Established
   Up/down time: 00:15:47
   Resets: 0
   Connection interface: GigabitEthernet2/1/2 (192.168.1.1)
   Received/sent messages: 16/16
   Discarded input messages: 0
   Discarded output messages: 0
   Elapsed time since last connection or counters clear: 00:17:40
   Mesh group peer joined: momo
   Last disconnect reason: Hold timer expired with truncated message
   Truncated packet: 5 bytes in buffer, type: 1, length: 20, without packet time: 75s
 Information about (Source, Group)-based SA filtering policy:
   Import policy: None
   Export policy: None
 Information about SA-Requests:
   Policy to accept SA-Requests: None
   Sending SA-Requests status: Disable
 Minimum TTL to forward SA with encapsulated data: 0
 SAs learned from this peer: 0, SA cache maximum for the peer: 4294967295
 Input queue size: 0, Output queue size: 0
 Counters for MSDP messages:
   RPF check failure: 0
   Incoming/outgoing SA: 0/0
   Incoming/outgoing SA-Request: 0/0
   Incoming/outgoing SA-Response: 0/0
   Incoming/outgoing Keepalive: 867/867
   Incoming/outgoing Notification: 0/0
   Incoming/outgoing Traceroutes in progress: 0/0
```

```
Incoming/outgoing Traceroute reply: 0/0
Incoming/outgoing Unknown: 0/0
Incoming/outgoing data packet: 0/0
```

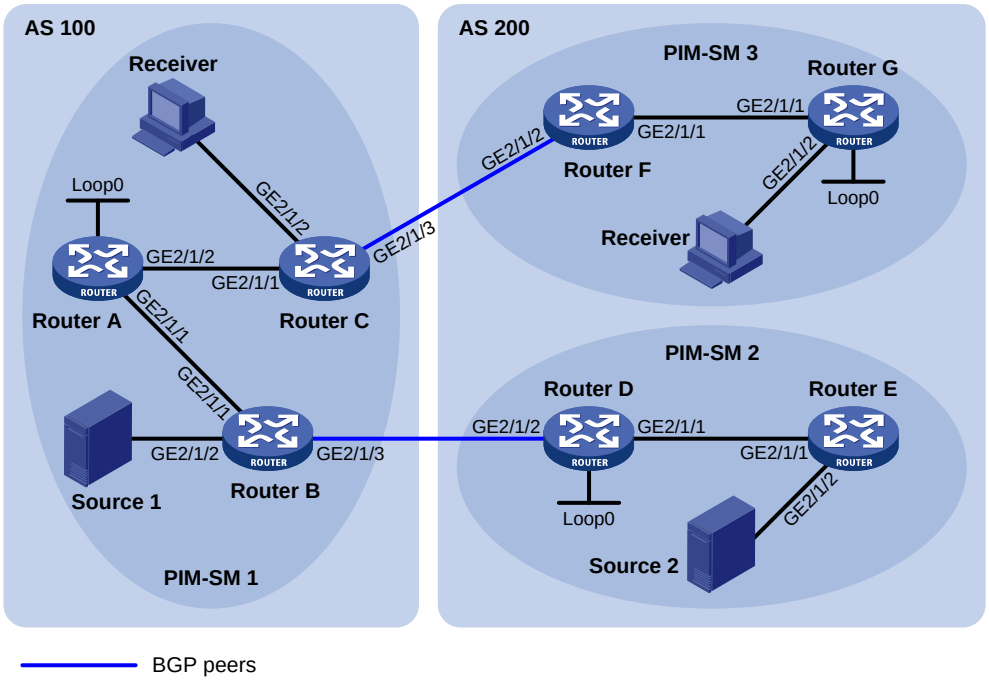
1.7.2 借助静态RPF对等体的AS间组播配置举例

1. 组网需求

- 网络中存在两个自治系统：AS 100 和 AS 200，各 AS 内部采用 OSPF 协议、AS 之间则采用 BGP 协议以保证单播路由的畅通；
- PIM-SM 1 属于 AS 100，PIM-SM 2 和 PIM-SM 3 属于 AS 200，每个 PIM-SM 域分别拥有至少一个组播源（Source）或接收者（Receiver）；
- 将 Router A、Router D 和 Router G 各自的 LoopBack0 接口分别配置为各自 PIM-SM 域的 C-BSR 和 C-RP；
- 根据 RPF 规则，设备接受来自其静态 RPF 对等体且被过滤策略所允许的 SA 报文。通过在各 PIM-SM 域的 RP 之间建立 MSDP 对等体，并在各 MSDP 对等体之间建立静态 RPF 对等体，从而在不改变单播拓扑的基础上实现各 PIM-SM 域之间组播源信息的共享。

2. 组网图

图1-6 借助静态 RPF 对等体的 AS 间组播配置组网图



设备	接口	IP地址	设备	接口	IP地址
Source 1	-	192.168.1.100/24	Router D	GE2/1/1	10.110.5.1/24
Source 2	-	192.168.3.100/24		GE2/1/2	10.110.3.2/24
Router A	GE2/1/1	10.110.1.1/24		Loop0	2.2.2.2/32
	GE2/1/2	10.110.2.1/24	Router E	GE2/1/1	10.110.5.2/24
	Loop0	1.1.1.1/32		GE2/1/2	192.168.3.1/24
Router B	GE2/1/1	10.110.1.2/24	Router F	GE2/1/1	10.110.6.1/24
	GE2/1/2	192.168.1.1/24		GE2/1/2	10.110.4.2/24
	GE2/1/3	10.110.3.1/24	Router G	GE2/1/1	10.110.6.2/24
Router C	GE2/1/1	10.110.2.2/24		GE2/1/2	192.168.4.1/24

	GE2/1/2	192.168.2.1/24		Loop0	3.3.3.3/32
	GE2/1/3	10.110.4.1/24			

3. 配置步骤

(1) 配置 IP 地址和单播路由协议

请按照 图 1-6 配置各接口的IP地址和掩码，具体配置过程略。

配置 AS 内的各路由器之间采用 OSPF 协议进行互连，确保 AS 内部在网络层互通，并且各路由器之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，使能 PIM-SM 和 IGMP，并配置 BSR 的服务边界

在 Router C 上使能 IP 组播路由，在主机侧接口 GigabitEthernet2/1/2 上使能 IGMP，并在其它接口上使能 PIM-SM。

```
<RouterC> system-view
[RouterC] multicast routing
[RouterC-mrib] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] pim sm
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface gigabitethernet 2/1/2
[RouterC-GigabitEthernet2/1/2] igmp enable
[RouterC-GigabitEthernet2/1/2] quit
[RouterC] interface gigabitethernet 2/1/3
[RouterC-GigabitEthernet2/1/3] pim sm
[RouterC-GigabitEthernet2/1/3] quit
```

Router A、Router B、Router D、Router E、Router F 和 Router G 上的配置与 Router C 相似，配置过程略。

在 Router B 上配置 BSR 的服务边界。

```
[RouterB] interface gigabitethernet 2/1/3
[RouterB-GigabitEthernet2/1/3] pim bsr-boundary
[RouterB-GigabitEthernet2/1/3] quit
```

Router C、Router D 和 Router F 上的配置与 Router B 相似，配置过程略。

(3) 配置 C-BSR 和 C-RP 的位置

在 Router A 上将 LoopBack0 接口配置为 C-BSR 和 C-RP。

```
[RouterA] pim
[RouterA-pim] c-bsr 1.1.1.1
[RouterA-pim] c-rp 1.1.1.1
[RouterA-pim] quit
```

Router D 和 Router G 上的配置与 Router A 相似，配置过程略。

(4) 配置 BGP 协议，将 BGP 与 OSPF 互相引入

在 Router B 上配置 EBGP 对等体，并引入 OSPF 路由。

```
[RouterB] bgp 100
[RouterB-bgp] router-id 1.1.1.2
[RouterB-bgp] peer 10.110.3.2 as-number 200
[RouterB-bgp] address-family ipv4 unicast
[RouterB-bgp-ipv4] peer 10.110.3.2 enable
```

```
[RouterB-bgp-ipv4] import-route ospf 1
[RouterB-bgp-ipv4] quit
[RouterB-bgp] quit
```

在 Router D 上配置 EBGP 对等体，并引入 OSPF 路由。

```
[RouterD] bgp 200
[RouterD-bgp] router-id 2.2.2.2
[RouterD-bgp] peer 10.110.3.1 as-number 100
[RouterD-bgp] address-family ipv4 unicast
[RouterD-bgp-ipv4] peer 10.110.3.1 enable
[RouterD-bgp-ipv4] import-route ospf 1
[RouterD-bgp-ipv4] quit
[RouterD-bgp] quit
```

在 Router C 上配置 EBGP 对等体，并引入 OSPF 路由。

```
[RouterC] bgp 100
[RouterC-bgp] router-id 1.1.1.3
[RouterC-bgp] peer 10.110.4.2 as-number 200
[RouterC-bgp] address-family ipv4 unicast
[RouterC-bgp-ipv4] peer 10.110.4.2 enable
[RouterC-bgp-ipv4] import-route ospf 1
[RouterC-bgp-ipv4] quit
[RouterC-bgp] quit
```

在 Router F 上配置 EBGP 对等体，并引入 OSPF 路由。

```
[RouterF] bgp 200
[RouterF-bgp] router-id 3.3.3.1
[RouterF-bgp] peer 10.110.4.1 as-number 100
[RouterF-bgp] address-family ipv4 unicast
[RouterF-bgp-ipv4] peer 10.110.4.1 enable
[RouterF-bgp-ipv4] import-route ospf 1
[RouterF-bgp-ipv4] quit
[RouterF-bgp] quit
```

在 Router B 的 OSPF 中引入 BGP。

```
[RouterB] ospf 1
[RouterB-ospf-1] import-route bgp
[RouterB-ospf-1] quit
```

在 Router D 的 OSPF 中引入 BGP。

```
[RouterD] ospf 1
[RouterD-ospf-1] import-route bgp
[RouterD-ospf-1] quit
```

在 Router C 的 OSPF 中引入 BGP。

```
[RouterC] ospf 1
[RouterC-ospf-1] import-route bgp
[RouterC-ospf-1] quit
```

在 Router F 的 OSPF 中引入 BGP。

```
[RouterF] ospf 1
[RouterF-ospf-1] import-route bgp
[RouterF-ospf-1] quit
```

(5) 配置 MSDP 对等体及静态 RPF 对等体

配置 Router D 和 Router G 作为 Router A 的 MSDP 对等体及静态 RPF 对等体。

```
[RouterA] ip prefix-list list-dg permit 10.110.0.0 16 greater-equal 16 less-equal 32
[RouterA] msdp
[RouterA-msdp] peer 10.110.3.2 connect-interface gigabitethernet 2/1/1
[RouterA-msdp] peer 10.110.6.2 connect-interface gigabitethernet 2/1/2
[RouterA-msdp] static-rpf-peer 10.110.3.2 rp-policy list-dg
[RouterA-msdp] static-rpf-peer 10.110.6.2 rp-policy list-dg
[RouterA-msdp] quit
```

配置 Router A 作为 Router D 的 MSDP 对等体及静态 RPF 对等体。

```
[RouterD] ip prefix-list list-a permit 10.110.0.0 16 greater-equal 16 less-equal 32
[RouterD] msdp
[RouterD-msdp] peer 10.110.1.1 connect-interface gigabitethernet 2/1/2
[RouterD-msdp] static-rpf-peer 10.110.1.1 rp-policy list-a
[RouterD-msdp] quit
```

配置 Router A 作为 Router G 的 MSDP 对等体及静态 RPF 对等体。

```
[RouterG] ip prefix-list list-a permit 10.110.0.0 16 greater-equal 16 less-equal 32
[RouterG] msdp
[RouterG-msdp] peer 10.110.2.1 connect-interface gigabitethernet 2/1/1
[RouterG-msdp] static-rpf-peer 10.110.2.1 rp-policy list-a
[RouterG-msdp] quit
```

4. 验证配置

通过使用 **display bgp peer** 命令可以查看路由器之间 BGP 对等体建立情况。Router A 上无任何信息输出，说明 Router A 与 Router D、Router A 与 Router G 之间均未建立 BGP 对等体关系。

当 PIM-SM 1 和 PIM-SM 2 域内的组播源 Source 1 和 Source 2 发送组播信息时，PIM-SM 1 和 PIM-SM 3 域内的接收者能收到该组播信息，通过使用 **display msdp brief** 命令可以查看路由器之间 MSDP 对等体的建立情况。例如：

显示 Router A 上 MSDP 对等体的简要信息。

```
[RouterA] display msdp brief
Configured   Established  Listen       Connect      Shutdown     Disabled
2            2            0            0            0            0

Peer address    State       Up/Down time    AS         SA count   Reset count
10.110.3.2      Established 01:07:08        ?          8          0
10.110.6.2      Established 00:16:39        ?          13         0
```

显示 Router D 上 MSDP 对等体的简要信息。

```
[RouterD] display msdp brief
Configured   Established  Listen       Connect      Shutdown     Disabled
1            1            0            0            0            0

Peer address    State       Up/Down time    AS         SA count   Reset count
10.110.1.1      Established 01:07:09        ?          8          0
```

显示 Router G 上 MSDP 对等体的简要信息。

```
[RouterG] display msdp brief
Configured   Established  Listen       Connect      Shutdown     Disabled
```

```
1           1           0           0           0           0

Peer address    State       Up/Down time    AS          SA count    Reset count
10.110.2.1      Established 00:16:40        ?           13          0
```

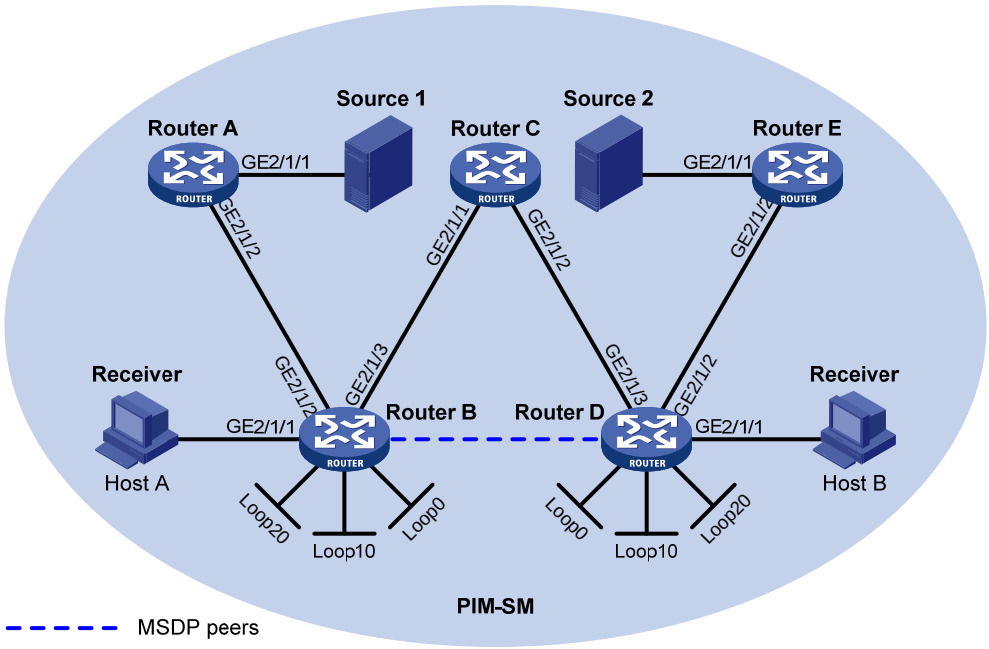
1.7.3 Anycast-RP应用配置举例

1. 组网需求

- PIM-SM 域内拥有多个组播源（Source）和接收者（Receiver），并在域内运行 OSPF 协议以提供单播路由；
- 通过配置 Anycast-RP，使接收者侧 DR 能够向拓扑距离最近的 RP 发起加入，组播源侧 DR 也向拓扑距离最近的 RP 发起注册；
- 将 Router B 和 Router D 各自的 LoopBack10 接口配置为 C-BSR、LoopBack20 接口配置为 C-RP；
- Router B 的 Router ID 为 1.1.1.1，Router D 的 Router ID 为 2.2.2.2，在 Router B 和 Router D 之间建立 MSDP 对等体关系。

2. 组网图

图1-7 Anycast-RP 应用配置组网图



设备	接口	IP地址	设备	接口	IP地址
Source 1	-	10.110.5.100/24	Router C	GE2/1/1	192.168.1.2/24
Source 2	-	10.110.6.100/24		GE2/1/2	192.168.2.2/24
Router A	GE2/1/1	10.110.5.1/24	Router D	GE2/1/1	10.110.3.1/24
	GE2/1/2	10.110.2.2/24		GE2/1/2	10.110.4.1/24
Router B	GE2/1/1	10.110.1.1/24		GE2/1/3	192.168.2.1/24
	GE2/1/2	10.110.2.1/24		Loop0	2.2.2.2/32
	GE2/1/3	192.168.1.1/24		Loop10	4.4.4.4/32
	Loop0	1.1.1.1/32		Loop20	10.1.1.1/32
	Loop10	3.3.3.3/32	Router E	GE2/1/1	10.110.6.1/24
	Loop20	10.1.1.1/32		GE2/1/2	10.110.4.2/24

3. 配置步骤

(1) 配置 IP 地址和单播路由协议

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。

配置 PIM-SM 域内的各路由器之间采用 OSPF 协议进行互连，确保 PIM-SM 域内部在网络层互通，并且各路由器之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，并使能 PIM-SM 和 IGMP

在 Router B 上使能 IP 组播路由，在主机侧接口 GigabitEthernet2/1/1 上使能 IGMP，并在其它接口上使能 PIM-SM。

```
<RouterB> system-view
[RouterB] multicast routing
[RouterB-mrib] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] igmp enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] pim sm
[RouterB-GigabitEthernet2/1/2] quit
[RouterB] interface gigabitethernet 2/1/3
[RouterB-GigabitEthernet2/1/3] pim sm
[RouterB-GigabitEthernet2/1/3] quit
[RouterB] interface loopback 0
[RouterB-LoopBack0] pim sm
[RouterB-LoopBack0] quit
[RouterB] interface loopback 10
[RouterB-LoopBack10] pim sm
[RouterB-LoopBack10] quit
[RouterB] interface loopback 20
[RouterB-LoopBack20] pim sm
[RouterB-LoopBack20] quit
```

Router A、Router C、Router D 和 Router E 上的配置与 Router B 相似，配置过程略。

(3) 配置 C-BSR 和 C-RP 的位置

在 Router B 上将 LoopBack10 配置为 C-BSR，将 LoopBack20 配置为 C-RP。

```
[RouterB] pim
[RouterB-pim] c-bsr 3.3.3.3
[RouterB-pim] c-rp 10.1.1.1
[RouterB-pim] quit
```

Router D 上的配置与 Router B 相似，配置过程略。

(4) 配置 MSDP 对等体

在 Router B 的 LoopBack0 接口上配置 MSDP 对等体。

```
[RouterB] msdp
[RouterB-msdp] originating-rp loopback 0
[RouterB-msdp] peer 2.2.2.2 connect-interface loopback 0
[RouterB-msdp] quit
```

在 Router D 的 LoopBack0 接口上配置 MSDP 对等体。

```
[RouterD] msdp
[RouterD-msdp] originating-rp loopback 0
[RouterD-msdp] peer 1.1.1.1 connect-interface loopback 0
[RouterD-msdp] quit
```

4. 验证配置

通过使用 **display msdp brief** 命令可以查看路由器之间 MSDP 对等体的简要信息。

显示 Router B 上 MSDP 对等体的简要信息。

```
[RouterB] display msdp brief
Configured   Established  Listen       Connect      Shutdown     Disabled
1          1          0         0         0         0

Peer address    State       Up/Down time    AS         SA count   Reset count
2.2.2.2         Established 00:00:13        ?          0          0
```

显示 Router D 上 MSDP 对等体的简要信息。

```
[RouterD] display msdp brief
Configured   Established  Listen       Connect      Shutdown     Disabled
1            1            0            0            0            0

Peer address    State       Up/Down time    AS         SA count   Reset count
1.1.1.1         Established 00:00:13        ?          0          0
```

通过使用 **display pim routing-table** 命令可以查看路由器上 PIM 路由表的内容。

当 Source 1（10.110.5.100/24）开始向组播组 G（225.1.1.1）发送组播信息时，Host A 加入组播组 G。通过比较 Router B 与 Router D 上 PIM 路由表的内容，可知当前的有效 RP 为 Router B：Source 1 向 Router B 注册，Host A 向 Router B 加入。

显示 Router B 上 PIM 路由表的内容。

```
[RouterB] display pim routing-table
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 225.1.1.1)
     RP: 10.1.1.1 (local)
     Protocol: pim-sm, Flag: WC
     UpTime: 00:15:04
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/1/1
             Protocol: igmp, UpTime: 00:15:04, Expires: -

 (10.110.5.100, 225.1.1.1)
     RP: 10.1.1.1 (local)
     Protocol: pim-sm, Flag: SPT 2MSDP ACT
     UpTime: 00:46:28
     Upstream interface: GigabitEthernet2/1/2
         Upstream neighbor: 10.110.2.2
```

```
        RPF prime neighbor: 10.110.2.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/1/1
            Protocol: pim-sm, UpTime:  - , Expires:  -
```

显示 Router D 上 PIM 路由表的内容。

```
[RouterD] display pim routing-table
```

Router D 上没有信息输出。

Host A 离开组播组 G，Source 1 也停止向组播组 G 发送组播数据。当 Source 2（10.110.6.100/24）开始向组播组 G 发送组播信息时，Host B 加入组播组 G。通过比较 Router B 与 Router D 上 PIM 路由的显示信息，可知当前的有效 RP 为 Router D：Source 2 向 Router D 注册，Host B 向 Router D 加入。

显示 Router B 上 PIM 路由表的内容。

```
[RouterB] display pim routing-table
```

Router B 上没有信息输出。

显示 Router D 上 PIM 路由表的内容。

```
[RouterD] display pim routing-table
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 225.1.1.1)
    RP: 10.1.1.1 (local)
    Protocol: pim-sm, Flag: WC
    UpTime: 00:12:07
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/1/1
            Protocol: igmp, UpTime: 00:12:07, Expires: -

 (10.110.6.100, 225.1.1.1)
    RP: 10.1.1.1 (local)
    Protocol: pim-sm, Flag: SPT 2MSDP ACT
    UpTime: 00:40:22
    Upstream interface: GigabitEthernet2/1/2
        Upstream neighbor: 10.110.4.2
        RPF prime neighbor: 10.110.4.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/1/1
            Protocol: pim-sm, UpTime:  - , Expires:  -
```

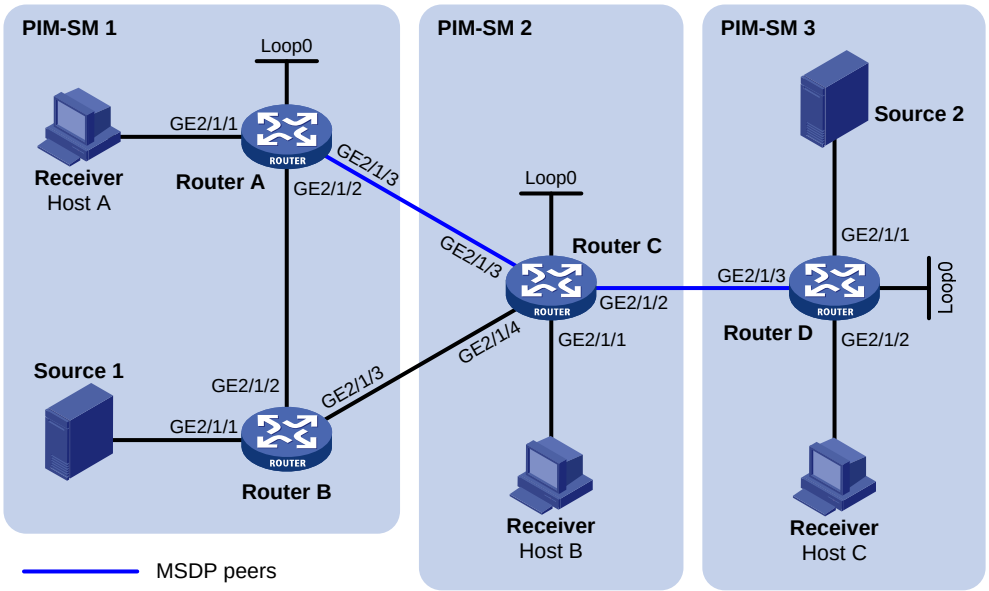
1.7.4 SA报文过滤机制配置举例

1. 组网需求

- 网络中存在三个 PIM-SM 域，各域内部以及域之间均运行 OSPF 协议以提供单播路由；
- 将 Router A、Router C 和 Router D 各自的 LoopBack0 接口分别配置为各自 PIM-SM 域的 C-BSR 和 C-RP；
- 分别在 Router A 与 Router C、Router C 与 Router D 之间建立 MSDP 对等体关系；
- 组播源 Source 1 向组播组 225.1.1.0/30 和 226.1.1.0/30 发送组播数据，组播源 Source 2 向组播组 227.1.1.0/30 发送组播数据；
- 通过配置 SA 报文过滤规则，使接收者 Host A 和 Host B 只能接收发往组播组 225.1.1.0/30 和 226.1.1.0/30 的组播数据，而 Host C 则只能接收发往组播组 226.1.1.0/30 和 227.1.1.0/30 的组播数据。

2. 组网图

图1-8 SA 报文过滤机制配置组网图



设备	接口	IP地址	设备	接口	IP地址
Source 1	-	10.110.3.100/24	Router C	GE2/1/1	10.110.4.1/24
Source 2	-	10.110.6.100/24		GE2/1/2	10.110.5.1/24
Router A	GE2/1/1	10.110.1.1/24		GE2/1/3	192.168.1.2/24
	GE2/1/2	10.110.2.1/24		GE2/1/4	192.168.2.2/24
	GE2/1/3	192.168.1.1/24		Loop0	2.2.2.2/32
	Loop0	1.1.1.1/32	Router D	GE2/1/1	10.110.6.1/24
Router B	GE2/1/1	10.110.3.1/24		GE2/1/2	10.110.7.1/24
	GE2/1/2	10.110.2.2/24		GE2/1/3	10.110.5.2/24
	GE2/1/3	192.168.2.1/24		Loop0	3.3.3.3/32

3. 配置步骤

(1) 配置 IP 地址和单播路由协议

请按照 图 1-8 配置各接口的IP地址和掩码，具体配置过程略。

配置各路由器之间采用 OSPF 协议进行互连，确保 PIM-SM 域内部以及各 PIM-SM 域之间在网络层互通，并且各路由器之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，使能 PIM-SM 和 IGMP，并配置 BSR 的服务边界

在 Router A 上使能 IP 组播路由，在主机侧接口 GigabitEthernet2/1/1 上使能 IGMP，并在其它接口上使能 PIM-SM。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] igmp enable
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] pim sm
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] interface gigabitethernet 2/1/3
[RouterA-GigabitEthernet2/1/3] pim sm
[RouterA-GigabitEthernet2/1/3] quit
[RouterA] interface loopback 0
[RouterA-LoopBack0] pim sm
[RouterA-LoopBack0] quit
```

Router B、Router C 和 Router D 上的配置与 Router A 相似，配置过程略。

在 Router C 上配置 BSR 的服务边界。

```
[RouterC] interface gigabitethernet 2/1/2
[RouterC-GigabitEthernet2/1/2] pim bsr-boundary
[RouterC-GigabitEthernet2/1/2] quit
[RouterC] interface gigabitethernet 2/1/3
[RouterC-GigabitEthernet2/1/3] pim bsr-boundary
[RouterC-GigabitEthernet2/1/3] quit
[RouterC] interface gigabitethernet 2/1/4
[RouterC-GigabitEthernet2/1/4] pim bsr-boundary
[RouterC-GigabitEthernet2/1/4] quit
```

Router A、Router B 和 Router D 上的配置与 Router C 相似，配置过程略。

(3) 配置 C-BSR 和 C-RP 的位置

在 Router A 上将 LoopBack0 接口配置为 C-BSR 和 C-RP。

```
[RouterA] pim
[RouterA-pim] c-bsr 1.1.1.1
[RouterA-pim] c-rp 1.1.1.1
[RouterA-pim] quit
```

Router C 和 Router D 上的配置与 Router A 相似，配置过程略。

(4) 配置 MSDP 对等体

在 Router A 上配置 MSDP 对等体。

```
[RouterA] msdp
[RouterA-msdp] peer 192.168.1.2 connect-interface gigabitethernet 2/1/3
[RouterA-msdp] quit
```

在 Router C 上配置 MSDP 对等体。

```
[RouterC] msdp
[RouterC-msdp] peer 192.168.1.1 connect-interface gigabitethernet 2/1/3
[RouterC-msdp] peer 10.110.5.2 connect-interface gigabitethernet 2/1/2
[RouterC-msdp] quit
```

在 Router D 上配置 MSDP 对等体。

```
[RouterD] msdp
[RouterD-msdp] peer 10.110.5.1 connect-interface gigabitethernet 2/1/3
[RouterD-msdp] quit
```

(5) 配置 SA 报文过滤规则

在 Router C 上配置不向 Router D 转发有关（Source 1，225.1.1.0/30）的 SA 报文。

```
[RouterC] acl number 3001
[RouterC-acl-adv-3001] rule deny ip source 10.110.3.100 0 destination 225.1.1.0 0.0.0.3
[RouterC-acl-adv-3001] rule permit ip source any destination any
[RouterC-acl-adv-3001] quit
[RouterC] msdp
[RouterC-msdp] peer 10.110.5.2 sa-policy export acl 3001
[RouterC-msdp] quit
```

在 Router D 上配置不创建有关 Source 2 的 SA 报文。

```
[RouterD] acl number 2001
[RouterD-acl-basic-2001] rule deny source 10.110.6.100 0
[RouterD-acl-basic-2001] quit
[RouterD] msdp
[RouterD-msdp] import-source acl 2001
[RouterD-msdp] quit
```

4. 验证配置

通过使用 **display msdp sa-cache** 命令可以查看路由器上 SA 缓存中的（S，G）表项信息。例如：

显示 Router C 上 SA 缓存中的（S，G）表项信息。

```
[RouterC] display msdp sa-cache
Total Source-Active Cache - 8 entries
Matched 8 entries

Source          Group           Origin RP       Pro  AS     Uptime   Expires
10.110.3.100    225.1.1.0       1.1.1.1         ?    ?      02:03:30 00:05:31
10.110.3.100    225.1.1.1       1.1.1.1         ?    ?      02:03:30 00:05:31
10.110.3.100    225.1.1.2       1.1.1.1         ?    ?      02:03:30 00:05:31
10.110.3.100    225.1.1.3       1.1.1.1         ?    ?      02:03:30 00:05:31
10.110.3.100    226.1.1.0       1.1.1.1         ?    ?      02:03:30 00:05:31
10.110.3.100    226.1.1.1       1.1.1.1         ?    ?      02:03:30 00:05:31
10.110.3.100    226.1.1.2       1.1.1.1         ?    ?      02:03:30 00:05:31
10.110.3.100    226.1.1.3       1.1.1.1         ?    ?      02:03:30 00:05:31
```

显示 Router D 上 SA 缓存中的（S，G）表项信息。

```
[RouterD] display msdp sa-cache
Total Source-Active Cache - 4 entries
Matched 4 entries

Source          Group           Origin RP       Pro  AS     Uptime   Expires
```

```
10.110.3.100    226.1.1.0       1.1.1.1         ?    ?      00:32:53 00:05:07
10.110.3.100    226.1.1.1       1.1.1.1         ?    ?      00:32:53 00:05:07
10.110.3.100    226.1.1.2       1.1.1.1         ?    ?      00:32:53 00:05:07
10.110.3.100    226.1.1.3       1.1.1.1         ?    ?      00:32:53 00:05:07
```

1.8 常见配置错误举例

1.8.1 MSDP对等体一直处于disabled状态

1. 故障现象

配置了 MSDP 对等体，但其状态一直显示为 disabled。

2. 分析

- 所配置的本地接口地址与 MSDP 对等体地址之间，建立起基于 TCP 连接的 MSDP 对等体关系；
- 如果本地接口地址与对端路由器上所配置的 MSDP 对等体地址不一致，TCP 连接就不会建立起来；
- 如果两个 MSDP 对等体之间没有路由，TCP 连接也不会建立起来。

3. 处理过程

(1) 检查各路由器之间的路由是否通达。通过命令 **display ip routing-table** 查看各路由器之间单播路由是否正确。

(2) 检查将成为 MSDP 对等体的两个路由器间是否存在到达对方的单播路由。

(3) 检查 MSDP 对等体之间的接口地址是否匹配。通过命令 **display current-configuration** 查看本地接口地址是否与对端 MSDP 对等体地址一致，应确保一致。

1.8.2 路由器SA缓存中没有SA表项

1. 故障现象

MSDP 没有将（S，G）转发项通过 SA 报文发送出去。

2. 分析

- 命令 **import-source** 用于控制将本域的（S，G）表项通过 SA 报文发送给 MSDP 对等体。如果没有指定参数 *acl-number* 则表示默认过滤掉所有的(S，G)表项，即不通告本域的所有(S，G）表项；
- 未配置 **import-source** 命令时，系统将发送本域的所有（S，G）信息。如果 MSDP 没有将本域的（S，G）表项通过 SA 报文发送出去，应检查 **import-source** 命令的配置是否正确。

3. 处理过程

(1) 检查各路由器之间的路由是否通达。通过命令 **display ip routing-table** 查看各路由器之间单播路由是否正确。

(2) 检查将成为 MSDP 对等体的两个路由器间是否存在到达对方的单播路由。

(3) 检查命令 **import-source** 及其参数 *acl-number* 的配置情况，确保 ACL 规则能够过滤合适的（S，G）信息。

1.8.3 Anycast-RP应用中RP间互通信息异常

1. 故障现象

在 Anycast-RP 的应用中，各 RP 之间没有互相交换其本地注册的（S，G）信息。

2. 分析

- 在 Anycast-RP 应用中，通过将同一 PIM-SM 域内的 RP 配置为 MSDP 对等体，可以实现 RP 间的冗余备份；
- MSDP 对等体地址不能与 Anycast-RP 地址相同，且 C-BSR 和 C-RP 必须配置在不同的设备或接口上；
- 在使用 **originating-rp** 命令进行配置后，MSDP 将利用该命令所指定的接口地址替换 SA 报文中的 RP 地址；
- 当 MSDP 对等体对收到的 SA 报文进行 RPF 检查时，如果发现 RP 地址为本地地址，将拒绝接收 SA 报文。

3. 处理过程

(1) 检查各路由器之间的路由是否通达。通过命令 **display ip routing-table** 查看各路由器之间单播路由是否正确。

(2) 检查将成为 MSDP 对等体的两个路由器间是否存在到达对方的单播路由。

(3) 检查 **originating-rp** 命令的配置情况。在 Anycast-RP 的应用环境中，一定要配置 **originating-rp** 命令，而且 **originating-rp** 命令所指定的接口地址要与建立 MSDP 对等体连接的本地接口地址相同。

(4) 检查所配置的 C-BSR 地址是否与 Anycast-RP 的地址不同，应确保两个地址不同。

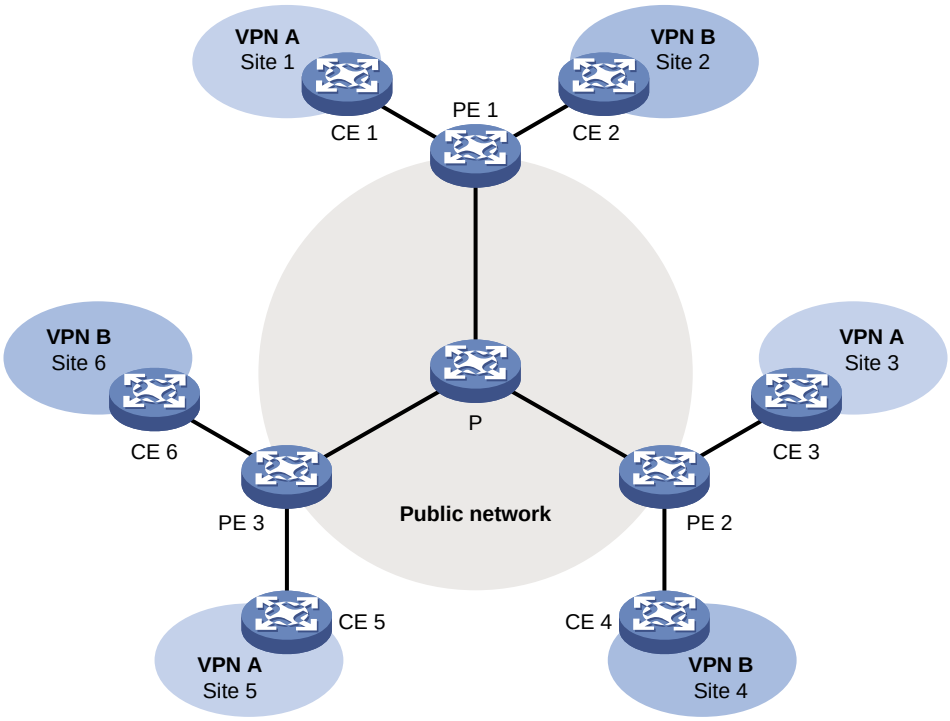
目　录

1 组播VPN

1.1 组播VPN简介

组播 VPN（Virtual Private Network，虚拟专用网络）是一项在 VPN 网络中实现组播传输的技术。

图1-1 典型的 VPN 组网



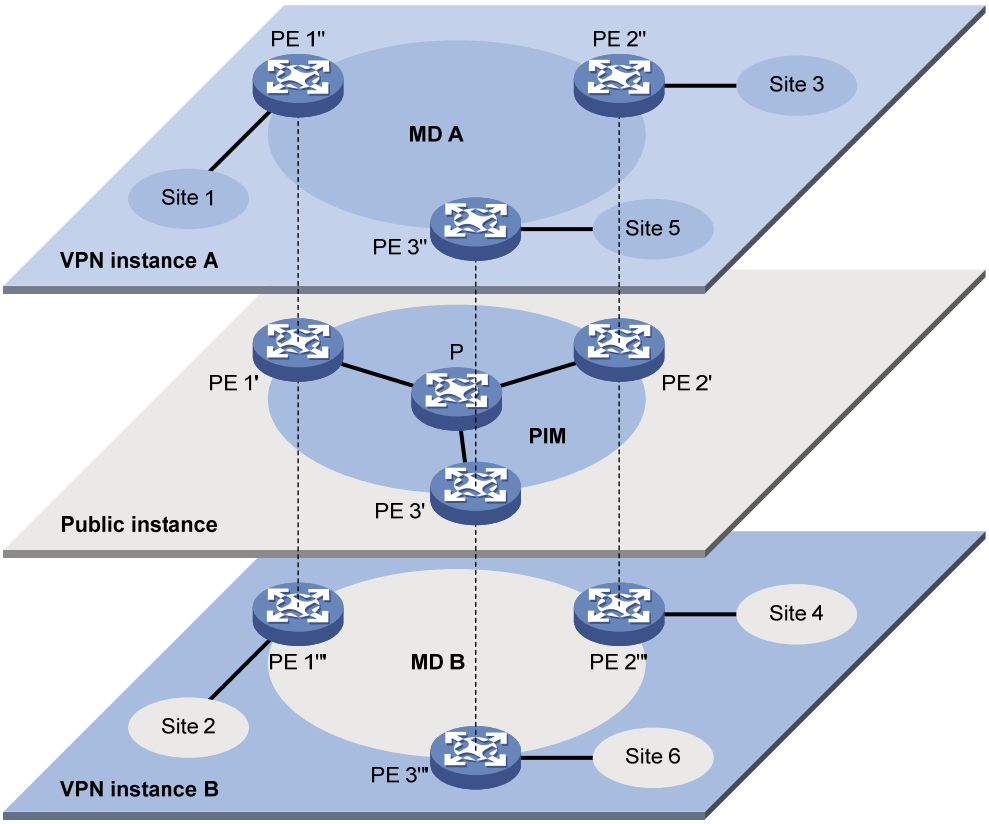
一个VPN网络由运营商的公共网络和用户的各个Site（站点）组成，各Site之间彼此相互孤立，只有借助公共网络才能实现互通。如 图 1-1 所示，由Site 1、Site 3 和Site 5 组成VPN A网络，由Site 2、Site 4 和Site 6 组成VPN B网络，其中包括以下三种类型的设备：

- P（Provider）：公共网络核心设备，不与 CE 直接相连。
- PE（Provider Edge）：公共网络边缘设备，与 CE 直接相连，负责 VPN 路由的处理。
- CE（Customer Edge）：用户网络边缘设备，可以是路由器或交换机，也可以是一台主机，负责用户网络路由的发布。

当 图 1-1 所示的VPN网络中运行组播VPN时，该网络中将同时承载着三个相互独立的组播业务：公网实例、VPN实例A和VPN实例B。公共网络边缘的PE组播设备支持多实例，相当于多台独立运行的组播设备。各实例之间形成彼此隔离的平面，每个实例对应一个平面，如 图 1-2 所示。

举例来说，图 1-1 中的PE 1 上运行着三个实例：公网实例、VPN实例A和VPN实例B，可以把这三个不同的实例想象成三台独立运行的虚拟设备，分别是PE 1’、PE 1”和PE 1”’，每台虚拟设备则分别对应着一个平面，对应关系如 图 1-2 所示。

图1-2 VPN 中基于多实例的组播



以 VPN 实例 A 为例，组播 VPN 是指：当 VPN A 中的组播源向某组播组发送组播数据时，在网络中所有可能的接收者中，只有属于 VPN A（即 Site 1、Site 3 或 Site 5 中）的组播组成员才能收到该组播源发来的组播数据。组播数据在各 Site 以及公网中均以组播方式进行传输。

由此分析，实现组播 VPN 所需具备的网络条件如下：

(1) 在每个 Site 内支持基于 VPN 实例的组播。

(2) 在公共网络内支持基于公网实例的组播。

(3) PE 支持多实例组播：

- 通过 VPN 实例连接 Site，支持基于 VPN 实例的组播；
- 通过公网实例连接公共网络，支持基于公网实例的组播；
- 支持公网实例与 VPN 实例之间的信息交流和数据转换。

Comware 利用 MD（Multicast Domain，组播域）方案来实现组播 VPN，简称为 MD VPN。该方案的最大优点就是仅需要 PE 支持多实例，而无需升级 CE 和 P，且无需修改 CE 和 P 上原有的 PIM 配置——也就是说，该方案对于 CE 和 P 是透明的。

1.1.2 MD VPN概述

1. MD VPN基本概念

MD VPN中所涉及到的基本概念如 表 1-1 所示。

表1-1 MD VPN 中的基本概念

概念	全称及中文解释	说明
MD	Multicast Domain，组播域	由各PE上能交互组播报文的相同VPN实例所构成的集合称为MD，不同的VPN实例属于不同的MD
MDT	Multicast Distribution Tree，组播分发树	建立在属于同一VPN内所有PE间的组播分发树，包括Default-MDT和Data-MDT两种
MT	Multicast Tunnel，组播隧道	在MD内将各PE连接到一起的通道称为MT，它用来传输MD内部的私网数据
MTI	Multicast Tunnel Interface，组播隧道接口	MTI是MT的入/出口，相当于MD的入/出口，PE通过MTI连接到MT上。MTI只收发组播报文，而不收发单播报文。MTI在创建VPN实例的MD时自动创建
Default-Group	默认组	每个MD在公网上分配一个独立的组播组，称为Default-Group。它是MD在公网上的唯一标志，用来在公网上建立MD所对应的Default-MDT
Default-MDT	Default-Multicast Distribution Tree，默认组播分发树	以Default-Group为组地址的MDT，称为Default-MDT。VPN使用Default-Group唯一标识一棵Default-MDT。Default-MDT是在配置完成后自动生成的，在公网中将会一直存在，而不论公网或私网中有没有实际的组播业务
Data-Group	数据组	当某私网组播数据的流量达到或超过阈值时，入口PE会为其分配一个独立的组播组，称为Data-Group，并通知其它PE使用该组播组在公网内转发该组播数据流量，从而实现Data-MDT切换
Data-MDT	Data-Multicast Distribution Tree，数据组播分发树	以Data-Group为组地址的MDT，称为Data-MDT。下游存在接收者的PE加入Data-Group，形成一棵Data-MDT，入口PE使用Data-MDT在公网中转发封装后的私网组播数据

2. MD VPN实现机制

MD VPN 实现机制的要点列举如下：

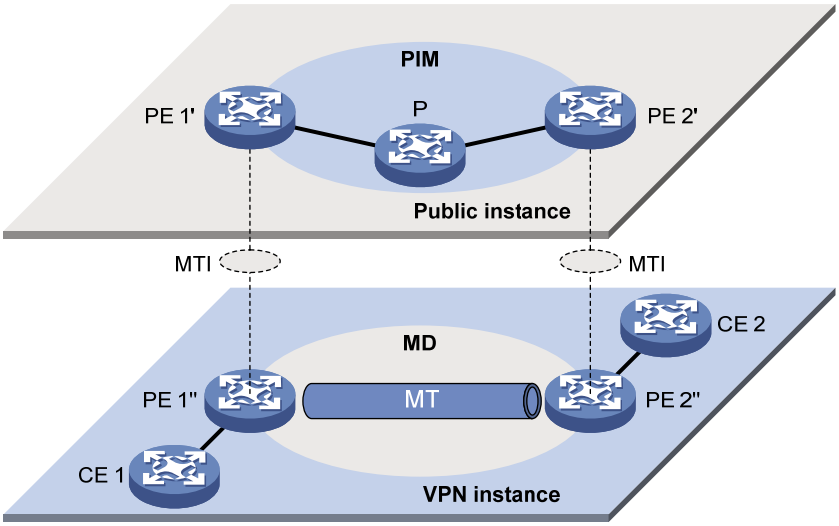
(1) 运营商构建的公共网络支持组播功能。PE 同时支持公网实例和多个 VPN 实例，每个实例各自运行相互间独立的 PIM。PE 与 CE 之间通过 VPN 实例进行私网组播传输；PE 与 P 之间则通过公网实例进行公网组播传输。

(2) MD在逻辑上表示某一特定VPN的私网组播数据在公网中的传播范围，在实际中则标识了网络中支持该VPN实例的所有PE。不同的VPN实例对应不同的MD。如 图 1-2 所示，其中每个VPN实例平面的中央椭圆区域表示一个MD，服务于某个特定的VPN，在该VPN中传输的所有私网组播数据，都在此MD内传输。

(3) 在 MD 内部，私网数据通过 MT 进行传输。MT 传输过程为：本地 PE 将私网组播报文封装成公网组播数据报文，并在公网内进行组播转发，远端 PE 收到该报文后通过解封装将其还原成私网报文。

(4) 本地PE将私网数据通过MTI发出，而远端PE则从MTI接收私网数据。如 图 1-3 所示，可以将MD比作一个私网数据的传输池，MTI则是MD的入/出口。本地PE将私网数据从入口（MTI）投入传输池，传输池自动将私网数据复制并传输到MD的所有出口（MTI），任何有需求的远端PE都可以从各自的出口（MTI）“打捞”私网数据。

图1-3 公网实例 PIM 与 VPN 实例 MD 对应关系示意图



(5) 一个 VPN 实例唯一对应一个 Default-Group。私网数据信息对于公网来说是透明的，不论私网组播报文属于哪个组播组、是协议报文还是数据报文，PE 都统一将其封装为普通的公网组播数据报文，并以 Default-Group 作为其所属的公网组播组。之后，PE 将封装好的公网组播数据报文发送到公网中。

(6) 一个 Default-Group 唯一对应一个 MD，并利用公网资源唯一创建一棵 Default-MDT 以进行数据转发。在该 VPN 中传输的所有私网组播报文，无论从哪个 PE 进入公网，都经由此 Default-MDT 转发。

(7) 一个 MD 唯一确定一个 Data-Group 范围以备进行 Data-MDT 切换。在进行 Data-MDT 切换时，从 Data-Group 范围中选取一个被引用最少的地址，从 PE 进入公网、流量达到或超过切换阈值的私网组播报文将使用该地址进行封装。

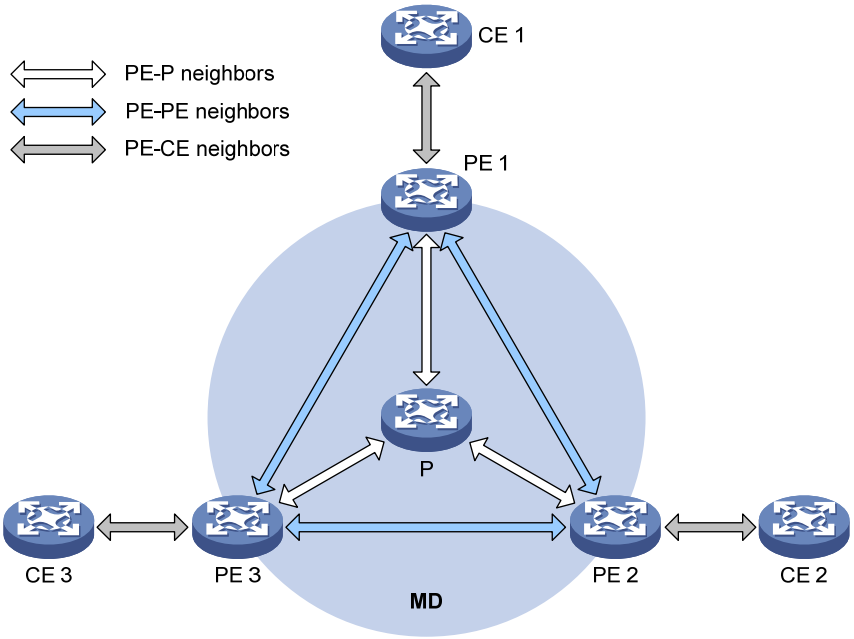
(8) 网络中所有 PE 都在监测私网组播数据流的转发速率，当某 PE 上私网组播数据流的转发速率超过阈值时，该 PE 将作为源端沿 Default-MDT 向其下游发出切换消息，使用 Data-Group 在该 PE 和有接收需求的远端 PE 之间新建一棵 Data-MDT。之后，进行 Data-MDT 切换：即从该 PE 进入公网的该私网组播数据流，不再使用 Default-Group 进行封装，而是被封装成公网的 Data-Group 组播报文，从 Default-MDT 切换到新创建的 Data-MDT 上。

说明

- 一个 VPN 唯一确定一个 MD，而一个 MD 也只能服务于一个 VPN，这种关系称为“一一对应”。VPN、MD、MTI、Default-Group 与 Data-Group 范围两两之间分别一一对应。
- 有关Data-MDT切换的详细介绍，请参见“1.2.3 Data-MDT切换”。

3. MD VPN中的PIM邻居关系

图1-4 MD VPN 中的 PIM 邻居关系示意图



PIM邻居关系建立在直接相连且属于同一网段的两台或多台设备之间。如 图 1-4 所示，在MD VPN中存在如下三种PIM邻居关系：

- PE-P 邻居关系：指 PE 上公网实例接口与链路对端 P 上的接口之间所建立的 PIM 邻居关系。
- PE-PE 邻居关系：指 PE 上的 VPN 实例通过 MTI 收到远端 PE 上的 VPN 实例发来的 PIM Hello 报文后所建立的邻居关系。
- PE-CE 邻居关系：指 PE 上绑定 VPN 实例的接口与链路对端 CE 上的接口之间所建立的 PIM 邻居关系。

1.1.3 协议规范

与组播 VPN 相关的协议规范有：

- RFC 6037：Cisco Systems' Solution for Multicast in BGP/MPLS IP VPNs

1.2 MD VPN实现原理

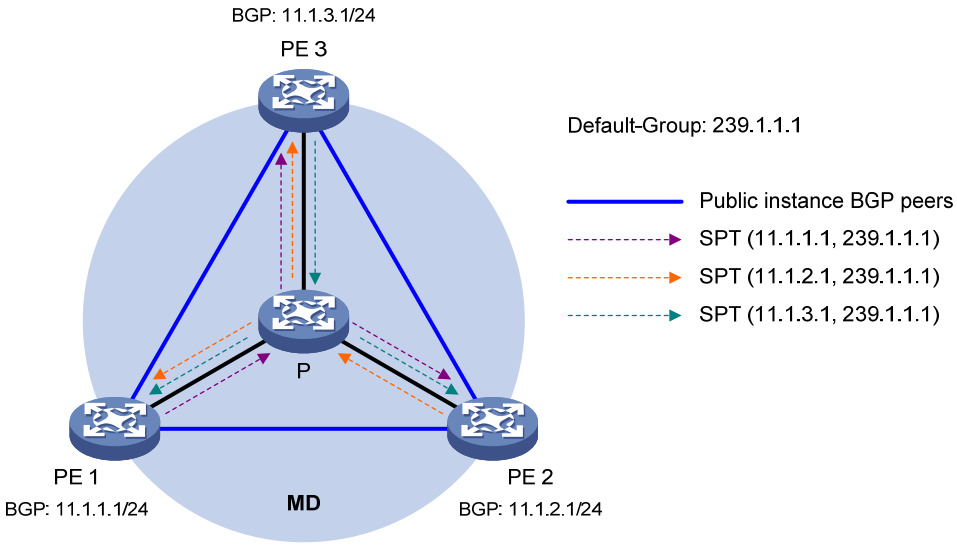
本节介绍 MD VPN 技术的实现原理，包括组播分发树的构建和工作过程，以及跨 AS 的实现方式。对于 VPN 实例来说，公网传输是透明的，私网数据的传输在 PE 上的 MTI 处完成了无缝连接：VPN 实例只知道将私网数据从 MTI 发出，然后远端就能从 MTI 接收。其实中间经历了复杂的公网传输过程，即 MDT 传输过程。

1.2.1 创建Default-MDT

公网中运行的组播路由协议可以是 PIM-DM 或 PIM-SM。在这两种情况下，创建 Default-MDT 的过程是有区别的。

1. 在PIM-DM网络中创建Default-MDT

图1-5 在 PIM-DM 网络中创建 Default-MDT



如 图 1-5 所示，公网中运行PIM-DM，PE 1、PE 2 和PE 3 都支持VPN实例A。Default-MDT的创建过程如下：

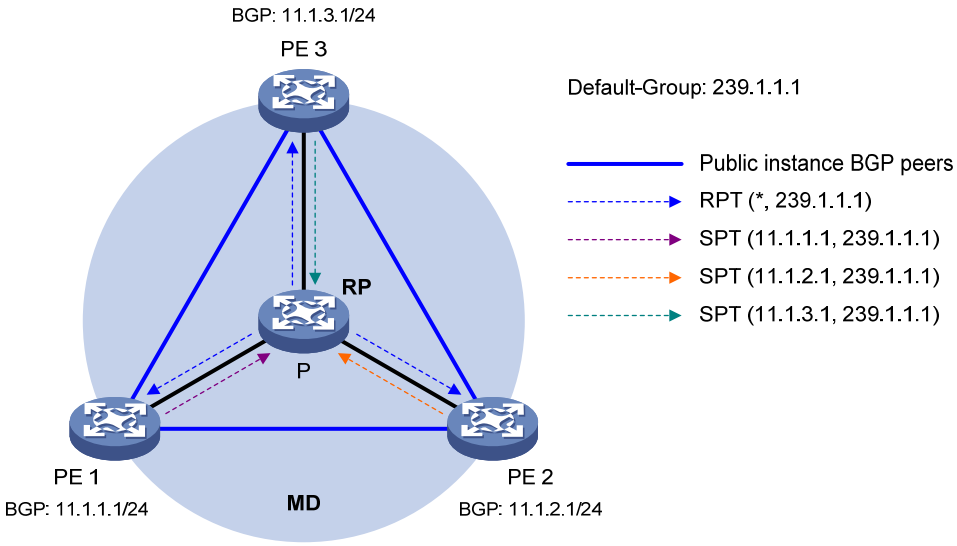
(1) PE 1 通过 VPN 实例 A 的 MTI 与其它 PE 建立 PIM 邻居关系时，会将私网 PIM 协议报文封装成公网组播数据报文（封装时以 MD 源接口的 IP 地址为源地址、Default-Group 为目的地址）在公网中发送。发送时，PE 1 以其它支持 VPN 实例 A 的 PE 为组播组成员，在整个公网范围内发起扩散—剪枝过程，在公网沿途各设备上分别创建（11.1.1.1，239.1.1.1）表项，从而形成一棵以 PE 1 为根、PE 2 和 PE 3 为叶的 SPT。

(2) 与此同时，PE 2 和 PE 3 也各自发起类似的扩散—剪枝过程，最终在 MD 中形成三棵相互独立的 SPT。

在 PIM-DM 网络中，由这三棵相互独立的 SPT 共同组成了一棵 Default-MDT。

2. 在PIM-SM网络中创建Default-MDT

图1-6 在 PIM-SM 网络中创建 Default-MDT



如 图 1-6 所示，公网中运行PIM-SM，PE 1、PE 2 和PE 3 都支持VPN实例A。Default-MDT的创建过程如下：

(1) PE 1 通过公网实例向公网 RP 发起（*，G）加入，以 Default-Group 为组播组地址，在公网沿途各设备上分别创建（*，239.1.1.1）表项。与此同时，PE 2 和 PE 3 也各自发起类似的加入过程，最终在 MD 中形成一棵以公网 RP 为根，PE 1、PE 2 和 PE 3 为叶的 RPT。

(2) PE 1 通过 VPN 实例 A 的 MTI 与其它 PE 建立 PIM 邻居关系时，会将私网 PIM 协议报文封装成公网组播数据报文（封装时以 MD 源接口的 IP 地址为源地址、Default-Group 为目的地址）在公网中发送。发送时，PE 1 先向公网 RP 发起注册过程，再由公网 RP 向 PE 1 发起加入，在公网沿途各设备上分别创建（11.1.1.1，239.1.1.1）表项。

(3) 与此同时，PE 2 和 PE 3 也各自发起类似的注册过程，最终在 MD 中形成三棵相互独立的、连接 PE 与 RP 的 SPT。

在 PIM-SM 网络中，由 RPT（*，239.1.1.1）和这三棵相互独立的 SPT 共同组成了一棵 Default-MDT。

3. Default-MDT的特点

综前所述，无论公网中运行的是何种 PIM 模式，Default-MDT 都具有以下特点：

- 网络中所有支持 VPN 实例 A 的 PE 都加入该 Default-MDT。
- 所有属于 VPN A 的私网组播报文进入公网后，均沿该 Default-MDT 向各 PE 转发，无论 PE 所连接的 Site 中是否存在接收者。

1.2.2 基于Default-MDT的传输

Default-MDT 构建完成后，就可以进行组播报文的传输。其中，组播协议报文和组播数据报文的传输过程是不同的，下面分别进行介绍。

1. 组播协议报文的传输

当私网组播协议报文需要跨越公网进行传输时，这些报文在本地 PE 上被封装为普通的公网组播数据并沿 Default-MDT 进行传输，在远端 PE 上被解封装，从而继续进行正常的协议交互过程，最终建立一棵跨越公网的组播分发树。组播协议报文的作用可分为以下几种情况：

(1) 当 VPN 网络中运行 PIM-DM 或 PIM-SSM 时：

- 各 MTI 之间通过交互 Hello 报文，建立 PIM 邻居。
- 通过跨越公网发起扩散—剪枝（PIM-DM）或加入（PIM-SSM）以创建 SPT。

(2) 当 VPN 网络中运行 PIM-SM 时：

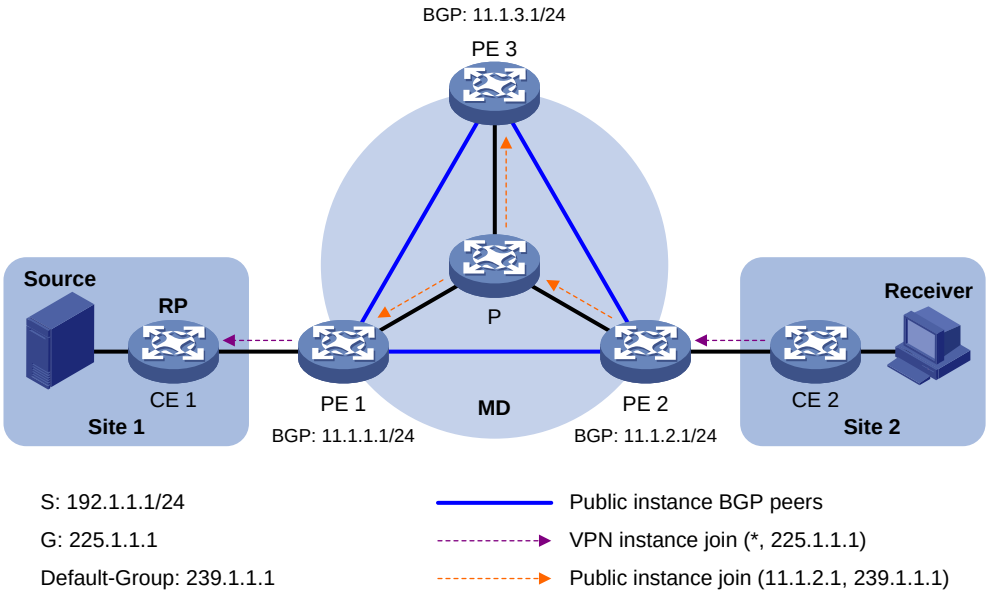
- 各 MTI 之间通过交互 Hello 报文，建立 PIM 邻居。
- 如果接收者与私网 RP 属于不同的 Site，通过跨越公网发起加入以创建 RPT。
- 如果组播源与私网 RP 属于不同的 Site，通过跨越公网发起注册以创建 SPT。

说明

- 在属于同一 VPN 的所有接口（包括 PE 上绑定 VPN 实例的接口和 MTI）上必须运行相同模式的 PIM 协议。
- 下面以公网和 VPN 网络中均运行 PIM-SM、私网接收者跨越公网发起加入为例，介绍基于 Default-MDT 的组播协议报文的传输过程。

如 图 1-7 所示，公网和VPN网络中分别运行PIM-SM，属于Site 2 的私网组播组G（225.1.1.1）的接收者（Receiver）与CE 2 相连；属于Site 1 的CE 1 作为G的RP；用于公网组播数据转发的Default-Group为 239.1.1.1。

图1-7 组播协议报文的传输过程



组播协议报文的交互过程如下：

(1) Receiver 向 CE 2 发送 IGMP 报告以加入组播组 G。CE 2 在本地创建（*，225.1.1.1）表项，同时向私网 RP（CE 1）发起加入。

(2) PE 2 上的 VPN 实例收到 CE 2 发来的加入消息后，在本地创建（*，225.1.1.1）表项，并指定 MTI 为上游接口，然后对该消息做进一步处理（详见第(3)步）。这时，PE 2 上的 VPN 实例将认为加入消息已从 MTI 发出。

(3) PE 2 对该加入消息进行 GRE（Generic Routing Encapsulation，通用路由封装）封装，以 MD 源接口的 IP 地址为源地址、Default-Group 为目的地址封装成公网组播数据报文（11.1.2.1，239.1.1.1），然后交给公网实例进行转发。

(4) 组播数据报文（11.1.2.1，239.1.1.1）沿 Default-MDT 传输给各 PE 上的公网实例。各 PE 将其解封装，还原为发往私网 RP 的加入消息，检查后如果发现要加入的私网 RP 位于本 Site，便将该消息交给 VPN 实例进行处理，否则将其丢弃。

(5) PE 1 上的 VPN 实例收到加入消息后，认为是从 MTI 获得的。在本地创建（*，225.1.1.1）表项，并指定 MTI 为下游接口、朝向 CE 1 的接口为上游接口。同时向私网 RP 发送加入消息。

(6) CE 1 收到 PE 1 上的 VPN 实例发来的加入消息后，在本地更新或创建（*，225.1.1.1）表项。至此跨越公网的 RPT 创建完成。

2. 组播数据报文的传输

当组播分发树创建完成后，组播源通过组播分发树将私网组播数据发送给各 Site 中的接收者。私网组播数据在本地 PE 上被封装为公网组播数据并沿 Default-MDT 传输，在远端 PE 上被解封装并继续在私网内传输。私网组播数据跨越公网的传输可分为以下几种情况：

(1) 当 VPN 网络中运行 PIM-DM 或 PIM-SSM 时，组播源通过私网 SPT 跨越公网向接收者发送私网组播数据。

(2) 当 VPN 网络中运行 PIM-SM 时：

- 在 SPT 切换前，如果组播源与私网 RP 属于不同的 Site，组播源先通过其与私网 RP 间的私网 SPT 跨越公网向私网 RP 发送私网组播数据；如果私网 RP 与接收者也属于不同的 Site，私网 RP 再通过私网 RPT 跨越公网向接收者继续转发私网组播数据。
- 在 SPT 切换后，如果组播源与接收者属于不同的 Site，组播源通过私网 SPT 跨越公网向接收者直接发送私网组播数据。

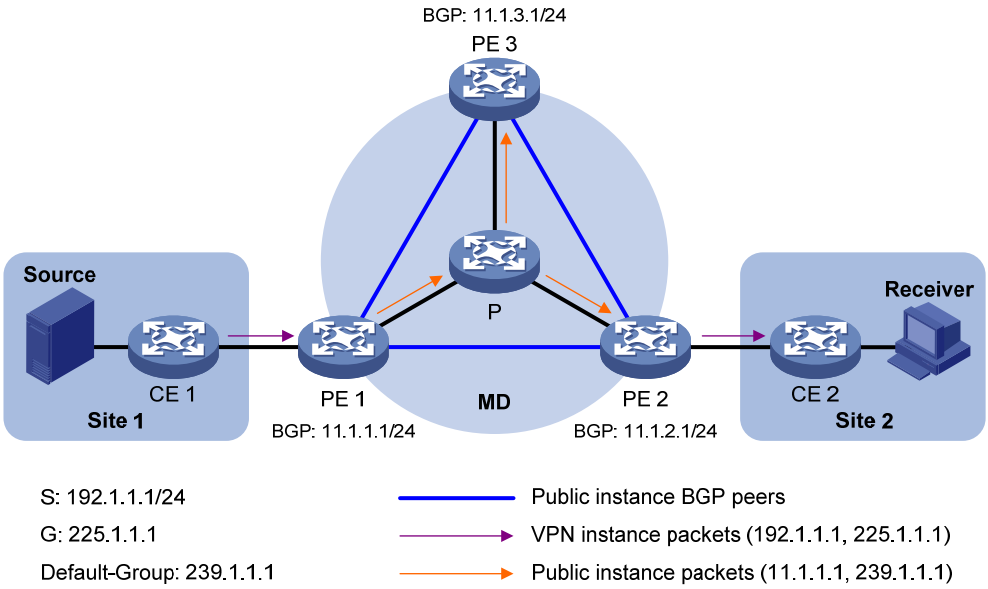
(3) 当 VPN 网络中运行双向 PIM 时，如果组播源与私网 RP 属于不同的 Site，组播源先通过其与私网 RP 间的私网组播源侧 RPT 跨越公网向私网 RP 发送私网组播数据；如果私网 RP 与接收者也属于不同的 Site，私网 RP 再通过私网接收者侧 RPT 跨越公网向接收者继续转发私网组播数据。

说明

- 有关 SPT 切换的详细介绍，请参见“IP 组播配置指导”中的“PIM”。
- 下面以公网和 VPN 网络中均运行 PIM-DM、沿私网 SPT 跨越公网传输私网组播数据为例，介绍基于 Default-MDT 的组播数据报文的传输过程。

如 图 1-8 所示，公网和VPN网络中分别运行PIM-DM，属于Site 2 的私网组播组G（225.1.1.1）的接收者（Receiver）与CE 2 相连；属于Site 1 的组播源（Source）向G发送组播数据；用于公网组播数据转发的Default-Group为 239.1.1.1。

图1-8 组播数据报文的传输过程



私网组播数据跨越公网进行传输的过程如下：

(1) Source 发送私网组播数据（192.1.1.1，225.1.1.1）到 CE 1。

(2) CE 1 沿 SPT 将私网组播数据转发给 PE 1，PE 1 上的 VPN 实例查找转发表项。如果对应转发表项的出接口列表中包含 MTI，则 PE 1 将对该私网组播数据做进一步处理（详见第(3)步）。这时，PE 1 上的 VPN 实例将认为私网组播数据已从 MTI 发出。

(3) PE 1 对该私网组播数据进行 GRE 封装，以 MD 源接口的 IP 地址为源地址、Default-Group 为目的地址封装成公网组播数据报文（11.1.1.1，239.1.1.1），然后交给公网实例进行转发。

(4) 组播数据报文（11.1.1.1，239.1.1.1）沿 Default-MDT 传输给各 PE 上的公网实例。各 PE 将其解封装，还原为私网组播数据，然后交给相应的 VPN 实例进行处理。如果该 PE 上存在 SPT 的下游接口，则沿 SPT 转发该私网组播数据，否则将其丢弃。

(5) PE 2 上的 VPN 实例查找转发表项，最终将私网组播数据送达 Receiver。至此跨越公网的私网组播数据传输完成。

1.2.3 Data-MDT切换

1. 由Default-MDT向Data-MDT切换

在公网中通过 Default-MDT 传送组播数据时，组播报文被传输到支持同一 VPN 实例的所有 PE 上，无论该 PE 所连接的 Site 内是否存在接收者。当私网中组播数据的传输速率比较大时，可能在公网中造成数据的泛滥。这样即浪费网络带宽，又增加了 PE 的处理负担。

为了解决上述问题，MD 方案对此进行了优化：为进入公网的大流量私网组播数据，在连接有私网接收者和私网组播源的各 PE 之间，建立起专用的 Data-MDT。然后将该组播数据流从 Default-MDT 切换到 Data-MDT，从而实现按需进行组播。

从 Default-MDT 向 Data-MDT 切换的过程如下：

(1) 源端 PE（如 PE 1）周期性地检测私网组播数据的转发速率。发起从 Default-MDT 向 Data-MDT 的切换必须同时满足以下两点要求：

- 私网组播数据通过了由 Default-MDT 向 Data-MDT 切换的 ACL 规则的过滤，否则仍沿 Default-MDT 转发；
- 私网组播数据的转发速率超过了切换阈值，且维持了一定的时间，否则仍沿 Default-MDT 转发。

(2) PE 1 从 Data-Group 范围中分配一个被引用最少的 Data-Group，沿 Default-MDT 向所有下游 PE 发送切换消息。该消息中包括私网组播源地址、私网组播组地址和 Data-Group。

(3) 其它 PE 收到该消息后，检查自己是否连接有该私网组播数据的接收者：如果有，则加入以 PE 1 为根的 Data-MDT；如果没有，则将该消息缓存起来，等待有接收者时再加入 Data-MDT。

(4) 当 PE 1 发送切换消息一定时间后，PE 1 停止使用 Default-Group 地址对私网组播数据进行封装，并改用 Data-Group 地址进行封装，组播数据沿 Data-MDT 向下分发。

(5) 当 Default-MDT 切换到 Data-MDT 之后，PE 1 会周期性地发送切换消息，以便后续有 PE 加入 Data-MDT。当某下游 PE 不再连接有接收者时，可以退出 Data-MDT。

说明

Data-MDT 和 Default-MDT 都是同一个 MD 中的转发隧道。Default-MDT 由 Default-Group 唯一确定；Data-MDT 则由 Data-Group 唯一确定。每个 Default-Group 关联一组 Data-Group 范围。

---

2. 由Data-MDT向Default-MDT反向切换

当私网组播数据切换到 Data-MDT 之后，由于情况变化而导致了不满足切换条件，PE 1 就会把此私网组播数据从 Data-MDT 反向切换回 Default-MDT，反向切换的触发条件包括（满足其一即可）：

- 私网组播数据转发速率低于指定切换阈值，且维持了一定的时间。
- 当更改了 Data-Group 范围后，用于私网组播数据封装的 Data-Group 被排除在新范围以外。
- 当控制私网组播数据由 Default-MDT 向 Data-MDT 切换的 ACL 规则发生了变化，从而导致私网组播数据不能通过新 ACL 规则的过滤。

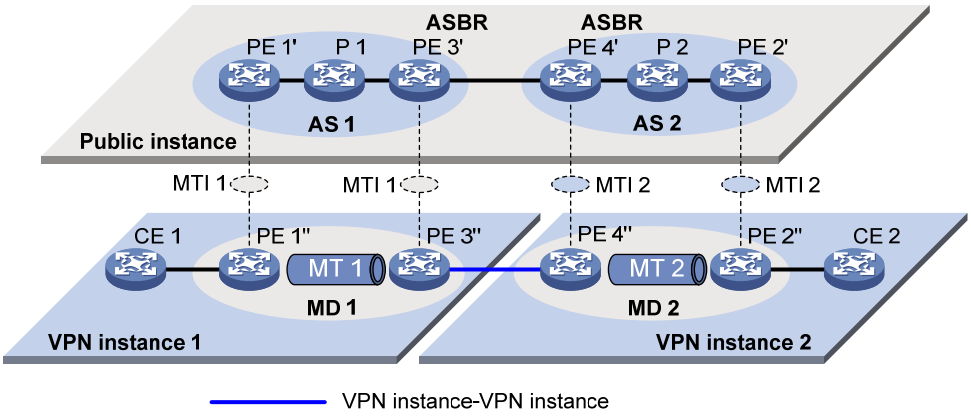
1.2.4 跨AS的MD VPN

当整个 VPN 跨越多个 AS（Autonomous System，自治系统）时，需要连通分布在不同 AS 内的各 VPN 节点。跨 AS 的 MD VPN 有以下两种实现方式：

1. VPN实例－VPN实例连接方式

如 图 1-9 所示，VPN跨越了AS 1 和AS 2 两个自治系统，PE 3 和PE 4 分别是AS 1 和AS 2 的ASBR。PE 3 和PE 4 通过各自的VPN实例相连，并互把对方视为CE设备。

图1-9 VPN 实例－VPN 实例连接方式示意图



采用 VPN 实例－VPN 实例方式时，需在每个 AS 内各建立一个独立的 MD，在各 MD 之间实现私网组播数据跨 AS 的传输。

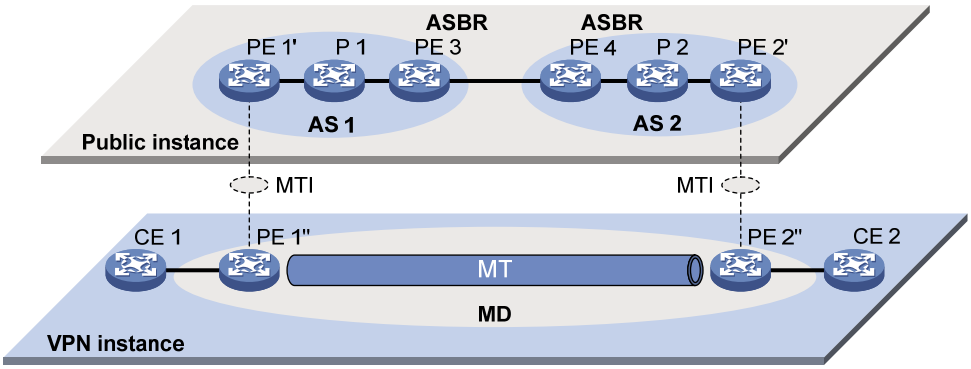
说明

由于 ASBR 之间转发的只是私网组播数据，因此各 AS 内部运行的公网 PIM 模式可以不同，但属于同一VPN的所有接口（包括ASBR上绑定VPN实例的接口）上必须运行统一的PIM模式（PIM-DM、PIM-SM、双向 PIM 或 PIM-SSM）。

2. Multi-hop EBGP连接方式

如图 1-10 所示，VPN跨越了AS 1和AS 2两个自治系统，PE 3和PE 4分别是AS 1和AS 2的ASBR。PE 3 和PE 4 通过各自的公网实例相连，并互把对方视为P设备。

图1-10 Multi-hop EBGP 连接方式



采用 Multi-hop EBGP 方式时，只需在所有 AS 内统一建立一个 MD 即可，在该 MD 内部实现公网组播数据跨 AS 的传输。

1.3 组播VPN配置任务简介

表1-2 组播 VPN 配置任务简介

配置任务		说明	详细配置
配置MD VPN	使能VPN实例中的IP组播路由	必选	1.4.2
	创建VPN实例的MD	必选	1.4.3
	指定Default-Group	必选	1.4.4
	指定MD源接口	必选	1.4.5
	配置Data-MDT切换参数	可选	1.4.6
	打开Data-Group重用日志输出开关	可选	1.4.7
配置BGP MDT	使能BGP MDT对等体/对等体组	必选	1.5.2
	配置BGP MDT路由反射器	可选	1.5.3

说明

MTI 无需用户手工创建，它随 MD 的创建而自动创建并与 VPN 实例绑定。需要注意的是：

- 只有在指定了 Default-Group 和 MD 源接口，并获取到 MD 源接口的公网 IP 地址之后，MTI 才会生效。
- MTI 上运行的 PIM 模式与其所属的 VPN 实例相同。只有当 VPN 实例中至少一个接口上使能了 PIM 协议，MTI 上的 PIM 协议才会被使能；当 VPN 实例中所有接口上都关闭了 PIM 协议，MTI 上的 PIM 协议也将被关闭。

1.4 配置MD VPN

1.4.1 配置准备

在配置 MD VPN 之前，需完成以下任务：

- 在公网中配置任一单播路由协议
- 在公网中配置 MPLS L3VPN
- 在公网中配置 PIM-DM 或 PIM-SM

在配置 MD VPN 之前，需准备以下数据：

- VPN 实例的名称和 RD（Route Distinguisher，路由标识符）
- Default-Group 的地址
- 建立 BGP 对等体时所使用的源接口
- Data-Group 的范围和切换条件

- Data-Group-Pool 的范围和切换条件
- 由 Default-MDT 向 Data-MDT 切换的延迟时间
- 由 Data-MDT 向 Default-MDT 反向切换的延迟时间

1.4.2 使能VPN实例中的IP组播路由

在配置 MD VPN 的各项功能之前，必须先创建 VPN 实例并使能该 VPN 实例中的 IP 组播路由。请在 PE 上进行本配置。

表1-3 使能 VPN 实例中的 IP 组播路由

操作	命令	说明
进入系统视图	**system-view**	-
创建VPN实例，并进入VPN实例视图	**ip vpn-instance** *vpn-instance-name*	缺省情况下，设备上不存在任何VPN实例 本命令请参见“MPLS命令参考”中的“MPLS L3VPN”
配置VPN实例的RD	**route-distinguisher** *route-distinguisher*	缺省情况下，VPN实例没有RD 本命令请参见“MPLS命令参考”中的“MPLS L3VPN”
退回系统视图	**quit**	-
使能VPN实例中的IP组播路由，并进入该VPN实例的MRIB视图	**multicast routing vpn-instance** *vpn-instance-name*	缺省情况下，IP组播路由处于关闭状态 本命令请参见“IP组播命令参考”中的“组播路由与转发”

1.4.3 创建VPN实例的MD

可以在 PE 上为一个或多个 VPN 实例创建其各自的 MD，来为不同的 VPN 提供服务。在创建 VPN 实例的 MD 时，系统会自动创建 MTI，并将其与该 VPN 实例绑定。

请在 PE 上进行本配置。

表1-4 创建 VPN 实例的 MD

操作	命令	说明
进入系统视图	**system-view**	-
创建指定VPN实例的MD，并进入MD视图	**multicast-domain vpn-instance** *vpn-instance-name*	缺省情况下，VPN实例不存在对应的MD

1.4.4 指定Default-Group

MTI 在封装私网组播报文时使用 Default-Group 作为目的地址。需要注意的是：

- 在不同的 PE 上，应该为相同 VPN 实例的 MD 指定相同的 Default-Group。
- 不允许指定已被其它 MD 使用的 Default-Group 或 Data-Group。

请在 PE 上进行本配置。

表1-5 指定 Default-Group

操作	命令	说明
进入系统视图	**system-view**	-
进入MD视图	**multicast-domain vpn-instance** *vpn-instance-name*	-
指定Default-Group	**default-group** *group-address*	缺省情况下，没有指定Default-Group

1.4.5 指定MD源接口

MTI 在封装私网组播报文时使用 MD 源接口的 IP 地址作为源地址。

需要注意的是，MD 源接口必须与建立 BGP 对等体时所使用的源接口相同，否则将无法获取正确的路由信息。

请在 PE 上进行本配置。

表1-6 指定 MD 源接口

操作	命令	说明
进入系统视图	**system-view**	-
进入MD视图	**multicast-domain vpn-instance** *vpn-instance-name*	-
指定MD源接口	**source** *interface-type interface-number*	缺省情况下，没有指定MD源接口

1.4.6 配置Data-MDT切换参数

在某些情况下，私网组播数据的转发速率会在切换阈值上下振荡。为了避免组播数据流在 Default-MDT 与 Data-MDT 之间进行频繁切换：

- 当转发速率高于阈值后并不立即切换，而是等待 Data-Delay 时间。在这段时间内如果转发速率始终高于阈值，则切换至 Data-MDT，否则继续使用 Default-MDT 进行转发；
- 当转发速率低于阈值后也不立即切换，而是等待 Data-Holddown 时间。在这段时间内如果转发速率始终低于阈值，则切换回 Default-MDT，否则继续使用 Data-MDT 进行转发。

请在 PE 上进行本配置。

表1-7 配置 Data-MDT 切换参数

操作	命令	说明
进入系统视图	**system-view**	-
进入MD视图	**multicast-domain vpn-instance** *vpn-instance-name*	-
配置Data-Group的范围和切换条件	**data-group** *group-address* { *mask-length* | *mask* } [**threshold** *threshold-value* | **acl** *acl-number*] *	缺省情况下，没有指定Data-Group的范围，也永不向Data-MDT进行切换
配置由Default-MDT向Data-MDT切换的延迟时间	**data-delay** *delay*	缺省情况下，由Default-MDT向Data-MDT切换的延迟时间为3秒
配置由Data-MDT向Default-MDT反向切换的延迟时间	**data-holddown** *delay*	缺省情况下，由Data-MDT向Default-MDT反向切换的延迟时间为60秒

1.4.7 打开Data-Group重用日志输出开关

在源 PE 上的 VPN 实例中，如果需要切换的私网组播数据流的个数超过了 Data-Group 范围中组地址的个数时，可以重复使用该地址池中的组地址。通过打开 Data-Group 重用日志输出开关可以记录组地址重用的日志信息。

说明

组地址重用日志信息的级别为 informational，隶属于 MD 模块。有关日志信息的详细介绍，请参见“网络管理和监控配置指导”中的“信息中心”。

请在 PE 上进行本配置。

表1-8 打开 Data-Group 重用日志输出开关

操作	命令	说明
进入系统视图	**system-view**	-
进入MD视图	**multicast-domain vpn-instance** *vpn-instance-name*	-
打开Data-Group重用日志输出开关	**log data-group-reuse**	缺省情况下，Data-Group重用日志输出开关处于关闭状态

1.5 配置BGP MDT

当在公网中运行 PIM-SSM 时，需要进行 BGP MDT 的配置。

1.5.1 配置准备

在配置 BGP MDT 之前，需完成以下任务：

- 在公网中配置 MPLS L3VPN
- 在公网中配置 BGP 基本功能
- 在公网中配置 PIM-SSM

在配置 BGP MDT 之前，需准备以下数据：

- MDT 对等体的 IP 地址
- 路由反射器的集群 ID

1.5.2 使能BGP MDT对等体/对等体组

只有在 BGP IPv4 MDT 地址族下使能 BGP MDT 对等体/对等体组后，本地路由器才能与指定的对等体/对等体组交换 MDT 信息，该信息包含 PE 地址及 PE 所在的 Default-Group 等信息。在公网中运行 PIM-SSM 时，组播 VPN 根据 MDT 信息在公网上建立以 PE 为根（即组播源）的 Default-MDT。请在 PE 上进行本配置。

表1-9 使能 BGP MDT 对等体/对等体组

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
创建BGP IPv4 MDT地址族，并进入BGP IPv4 MDT地址族视图	**address-family ipv4 mdt**	缺省情况下，没有创建BGP IPv4 MDT地址族
使能本地路由器与指定对等体/对等体组交换MDT路由信息的能力	**peer** { *group-name* | *ip-address* } **enable**	缺省情况下，本地路由器不具有与指定对等体/对等体组交换MDT路由信息的能力 本命令的详细介绍，请参见“三层技术-IP路由命令参考”中的“BGP” 在执行本命令前，需先在BGP视图下创建对等体/对等体组，创建方法请参见“三层技术-IP路由配置指导”中的“BGP”

1.5.3 配置BGP MDT路由反射器

为保证位于同一 AS 内的 BGP MDT 对等体间的连通性，需要在对等体之间建立全连接关系，而当对等体的数目很多时，建立全连接的开销很大，使用路由反射器则可以解决这个问题。

在配置了路由反射器之后，其它路由器作为客户机与路由反射器建立 BGP 会话，路由反射器在客户机之间传递（反射）BGP MDT 信息，从而使各客户机之间无需建立 BGP 会话。

如果配置了路由反射器后，由于组网需要在路由反射器的客户机之间建立了全连接，则客户机之间可以直接交换路由信息，客户机到客户机之间的路由反射是没有必要的。此时，不需要修改网络配置或改变网络拓扑，只需在路由反射器上通过 **undo reflect between-clients** 命令禁止其在客户机之间反射路由，就可以避免路由反射，减少占用的带宽资源。

路由反射器及其客户机共同组成了一个集群。通常，一个集群中只有一个路由反射器，并通过其 Router ID 来识别该集群。为了增强网络的可靠性，可在一个集群中配置多个路由反射器，此时应为每个路由反射器配置相同的集群 ID，以避免产生路由环路。

请在 PE 上进行本配置。本配置中各命令的详细介绍，请参见“三层技术-IP 路由命令参考”中的“BGP”。

表1-10 配置 BGP MDT 路由反射器

操作	命令	说明
进入系统视图	**system-view**	-
进入BGP视图	**bgp** *as-number*	-
进入BGP IPv4 MDT地址族视图	**address-family ipv4 mdt**	-
配置本机作为路由反射器，对等体/对等体组作为路由反射器的客户机	**peer** { *group-name* | *ip-address* } **reflect-client**	缺省情况下，没有配置路由反射器及其客户机
（可选）禁止路由反射器在客户机之间反射路由	**undo reflect between-clients**	缺省情况下，允许路由反射器在客户机之间反射路由
（可选）配置路由反射器的集群ID	**reflector cluster-id** { *cluster-id* | *ip-address* }	缺省情况下，每个路由反射器都使用自己的Router ID作为集群ID

1.6 组播VPN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 VPN 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** 命令可以复位 MDT 地址族下的 BGP 会话。

表1-11 组播 VPN 显示和维护

操作	命令
显示BGP MDT对等体组的信息	**display bgp group ipv4 mdt** [**group-name** *group-name*]
显示BGP MDT对等体或对等体组的信息	**display bgp peer ipv4 mdt** [{ *ip-address* | **group-name** *group-name* } **log-info** | [*ip-address*] **verbose**]
显示BGP MDT的路由信息	**display bgp routing-table ipv4 mdt** [**route-distinguisher** *route-distinguisher*] [*ip-address* [**advertise-info**]]
显示BGP IPv4 MDT地址族下打包组的相关信息	**display bgp update-group ipv4 mdt** [*ip-address*]
显示MD中收到的Data-Group信息	**display multicast-domain vpn-instance** *vpn-instance-name* **data-group receive** [**brief** | [**active** | **group** *group-address* | **sender** *source-address* | *vpn-source-address* [**mask** { *mask-length* | *mask* }] | *vpn-group-address* [**mask** { *mask-length* | *mask* }]] *]
显示MD中发送的Data-Group信息	**display multicast-domain vpn-instance** *vpn-instance-name* **data-group send** [**group** *group-address* | **reuse** *interval* | *vpn-source-address* [**mask** { *mask-length* | *mask* }] | *vpn-group-address* [**mask** { *mask-length* | *mask* }]] *
显示Default-Group的信息	**display multicast-domain** [**vpn-instance** *vpn-instance-name*] **default-group** { **local** | **remote** }
复位MDT地址族下的BGP会话	**reset bgp** { *as-number* | *ip-address* | **all** | **external** | **group** *group-name* | **internal** } **ipv4 mdt**

说明

有关 **display bgp group**、**display bgp peer**、**display bgp update-group** 和 **reset bgp** 命令的详细介绍，请参见“三层技术-IP 路由命令参考”中的“BGP”。

1.7 组播VPN典型配置举例

1.7.1 单AS内MD VPN配置举例

1. 组网需求

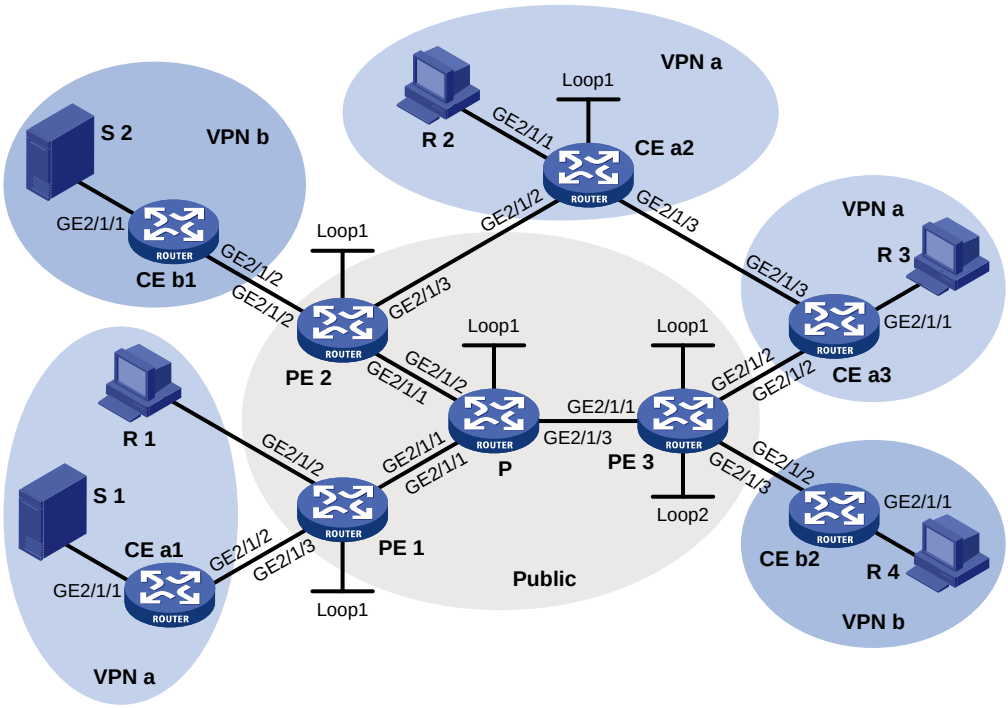
组网需求如 表 1-12 所示。

表1-12 单 AS 内 MD VPN 配置组网需求

项目	组网需求
组播源和接收者	• VPN a 中的组播源为 S 1，接收者为 R 1、R 2 和 R 3 • VPN b 中的组播源为 S 2，接收者为 R 4 • VPN a 中的 Default-Group 为 239.1.1.1，Data-Group 范围为 225.2.2.0～225.2.2.15 • VPN b 中的 Default-Group 为 239.2.2.2，Data-Group 范围为 225.4.4.0～225.4.4.15
PE上各接口所属的VPN实例	• PE 1：GigabitEthernet2/1/2 和 GigabitEthernet2/1/3 属于 VPN 实例 a，GigabitEthernet2/1/1 和 LoopBack1 属于公网实例 • PE 2：GigabitEthernet2/1/2 属于 VPN 实例 b，GigabitEthernet2/1/3 属于 VPN 实例 a，GigabitEthernet2/1/1 和 LoopBack1 属于公网实例 • PE 3：GigabitEthernet2/1/2 属于 VPN 实例 a，GigabitEthernet2/1/3 和 LoopBack2 属于 VPN 实例 b，GigabitEthernet2/1/1 和 LoopBack1 接口属于公网实例
单播路由协议和MPLS	• 在公网中配置 OSPF，在各 PE 与 CE 之间配置 RIP • 在 PE 1、PE 2 和 PE 3 各自的 LoopBack1 接口之间建立 BGP 对等体连接并传递所有私网路由 • 在公网中配置 MPLS
IP组播路由功能	• 在 P 上使能 IP 组播路由 • 在 PE 1、PE 2 和 PE 3 的公网实例中均使能 IP 组播路由 • 在 PE 1、PE 2 和 PE 3 的 VPN 实例 a 中均使能 IP 组播路由 • 在 PE 2 和 PE 3 的 VPN 实例 b 中均使能 IP 组播路由 • 在 CE a1、CE a2、CE a3、CE b1 和 CE b2 上均使能 IP 组播路由
IGMP功能	• 在 PE 1 的 GigabitEthernet2/1/2 接口上使能 IGMPv2 • 在 CE a2、CE a3 和 CE b2 各自的 GigabitEthernet2/1/1 接口上均使能 IGMPv2
PIM功能	• 在 P 的所有接口上均使能 PIM-SM • 在 PE 1、PE 2 和 PE 3 的所有不连接接收者的公网和私网接口上均使能 PIM-SM • 在 CE a1、CE a2、CE a3、CE b1 和 CE b2 的所有不连接接收者的接口上均使能 PIM-SM • P 的 LoopBack1 接口为公网的 C-BSR 和 C-RP（服务于所有组播组） • CE a2 的 LoopBack1 接口为 VPN a 的 C-BSR 和 C-RP（服务于所有组播组） • PE 3 的 LoopBack2 接口为 VPN b 的 C-BSR 和 C-RP（服务于所有组播组）

2. 组网图

图1-11 单 AS 内 MD VPN 配置组网图



设备	接口	IP地址	设备	接口	IP地址
S 1	-	10.110.7.2/24	PE 3	GE2/1/1	192.168.8.1/24
S 2	-	10.110.8.2/24		GE2/1/2	10.110.5.1/24
R 1	-	10.110.1.2/24		GE2/1/3	10.110.6.1/24
R 2	-	10.110.9.2/24		Loop1	1.1.1.3/32
R 3	-	10.110.10.2/24		Loop2	33.33.33.33/32
R 4	-	10.110.11.2/24	CE a1	GE2/1/1	10.110.7.1/24
P	GE2/1/1	192.168.6.2/24		GE2/1/2	10.110.2.2/24
	GE2/1/2	192.168.7.2/24	CE a2	GE2/1/1	10.110.9.1/24
	GE2/1/3	192.168.8.2/24		GE2/1/2	10.110.4.2/24
	Loop1	2.2.2.2/32		GE2/1/3	10.110.12.1/24
PE 1	GE2/1/1	192.168.6.1/24		Loop1	22.22.22.22/32
	GE2/1/2	10.110.1.1/24	CE a3	GE2/1/1	10.110.10.1/24
	GE2/1/3	10.110.2.1/24		GE2/1/2	10.110.5.2/24
	Loop1	1.1.1.1/32		GE2/1/3	10.110.12.2/24
PE 2	GE2/1/1	192.168.7.1/24	CE b1	GE2/1/1	10.110.8.1/24
	GE2/1/2	10.110.3.1/24		GE2/1/2	10.110.3.2/24
	GE2/1/3	10.110.4.1/24	CE b2	GE2/1/1	10.110.11.1/24
	Loop1	1.1.1.2/32		GE2/1/2	10.110.6.2/24

3. 配置步骤

(1) 配置 PE 1

配置全局 Router ID，并使能公网实例中的 IP 组播路由。

```
<PE1> system-view
[PE1] router id 1.1.1.1
[PE1] multicast routing
[PE1-mrib] quit
```

配置 LSR ID，并全局使能 LDP 能力。

```
[PE1] mpls lsr-id 1.1.1.1
```

```
[PE1] mpls ldp
[PE1-ldp] quit
```
创建 VPN 实例 a，并为其配置 RD 和 Route Target。
```
[PE1] ip vpn-instance a
[PE1-vpn-instance-a] route-distinguisher 100:1
[PE1-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE1-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE1-vpn-instance-a] quit
```
使能 VPN 实例 a 中的 IP 组播路由。
```
[PE1] multicast routing vpn-instance a
[PE1-mrib-a] quit
```
创建 VPN 实例 a 的 MD，并指定 Default-Group、MD 源接口和 Data-Group 范围。
```
[PE1] multicast-domain vpn-instance a
[PE1-md-a] default-group 239.1.1.1
[PE1-md-a] source loopback 1
[PE1-md-a] data-group 225.2.2.0 28
[PE1-md-a] quit
```
在公网接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 PIM-SM、MPLS 能力和 LDP 能力。
```
[PE1] interface gigabitethernet 2/1/1
[PE1-GigabitEthernet2/1/1] ip address 192.168.6.1 24
[PE1-GigabitEthernet2/1/1] pim sm
[PE1-GigabitEthernet2/1/1] mpls enable
[PE1-GigabitEthernet2/1/1] mpls ldp enable
[PE1-GigabitEthernet2/1/1] quit
```
将接口 GigabitEthernet2/1/2 与 VPN 实例 a 进行关联，配置 IP 地址，并使能 IGMP。
```
[PE1] interface gigabitethernet 2/1/2
[PE1-GigabitEthernet2/1/2] ip binding vpn-instance a
[PE1-GigabitEthernet2/1/2] ip address 10.110.1.1 24
[PE1-GigabitEthernet2/1/2] igmp enable
[PE1-GigabitEthernet2/1/2] quit
```
将接口 GigabitEthernet2/1/3 与 VPN 实例 a 进行关联，配置 IP 地址，并使能 PIM-SM。
```
[PE1] interface gigabitethernet 2/1/3
[PE1-GigabitEthernet2/1/3] ip binding vpn-instance a
[PE1-GigabitEthernet2/1/3] ip address 10.110.2.1 24
[PE1-GigabitEthernet2/1/3] pim sm
[PE1-GigabitEthernet2/1/3] quit
```
配置 LoopBack1 接口的 IP 地址，并使能 PIM-SM。
```
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 1.1.1.1 32
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```
配置 BGP 协议。
```
[PE1] bgp 100
[PE1-bgp] group vpn-g internal
[PE1-bgp] peer vpn-g connect-interface loopback 1
[PE1-bgp] peer 1.1.1.2 group vpn-g
```

```
[PE1-bgp] peer 1.1.1.3 group vpn-g
[PE1–bgp] ip vpn-instance a
[PE1-bgp-a] address-family ipv4
[PE1-bgp-ipv4-a] import-route rip 2
[PE1-bgp-ipv4-a] import-route direct
[PE1-bgp-ipv4-a] quit
[PE1-bgp-a] quit
[PE1–bgp] address-family vpnv4
[PE1–bgp-vpnv4] peer vpn-g enable
[PE1–bgp-vpnv4] quit
[PE1–bgp] quit
```

配置 OSPF 协议。

```
[PE1] ospf 1
[PE1-ospf-1] area 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.255.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 RIP 协议。

```
[PE1] rip 2 vpn-instance a
[PE1-rip-2] network 10.0.0.0
[PE1-rip-2] import-route bgp
[PE1-rip-2] return
```

(2) 配置 PE 2

配置全局 Router ID，并使能公网实例中的 IP 组播路由。

```
<PE2> system-view
[PE2] router id 1.1.1.2
[PE2] multicast routing
[PE2-mrib] quit
```

配置 LSR ID，并全局使能 LDP 能力。

```
[PE2] mpls lsr-id 1.1.1.2
[PE2] mpls ldp
[PE2-ldp] quit
```

创建 VPN 实例 b，并为其配置 RD 和 Route Target。

```
[PE2] ip vpn-instance b
[PE2-vpn-instance-b] route-distinguisher 200:1
[PE2-vpn-instance-b] vpn-target 200:1 export-extcommunity
[PE2-vpn-instance-b] vpn-target 200:1 import-extcommunity
[PE2-vpn-instance-b] quit
```

使能 VPN 实例 b 中的 IP 组播路由。

```
[PE2] multicast routing vpn-instance b
[PE2-mrib-b] quit
```

创建 VPN 实例 b 的 MD，并指定 Default-Group、MD 源接口和 Data-Group 范围。

```
[PE2] multicast-domain vpn-instance b
[PE2-md-b] default-group 239.2.2.2
[PE2-md-b] source loopback 1
```

```
[PE2-md-b] data-group 225.4.4.0 28
[PE2-md-b] quit
```
创建 VPN 实例 a，并为其配置 RD 和 Route Target。
```
[PE2] ip vpn-instance a
[PE2-vpn-instance-a] route-distinguisher 100:1
[PE2-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE2-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE2-vpn-instance-a] quit
```
使能 VPN 实例 a 中的 IP 组播路由。
```
[PE2] multicast routing vpn-instance a
[PE2-mrib-a] quit
```
创建 VPN 实例 a 的 MD，并指定 Default-Group、MD 源接口和 Data-Group 范围。
```
[PE2] multicast-domain vpn-instance a
[PE2-md-a] default-group 239.1.1.1
[PE2-md-a] source loopback 1
[PE2-md-a] data-group 225.2.2.0 28
[PE2-md-a] quit
```
在公网接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 PIM-SM、MPLS 能力和 LDP 能力。
```
[PE2] interface gigabitethernet 2/1/1
[PE2-GigabitEthernet2/1/1] ip address 192.168.7.1 24
[PE2-GigabitEthernet2/1/1] pim sm
[PE2-GigabitEthernet2/1/1] mpls enable
[PE2-GigabitEthernet2/1/1] mpls ldp enable
[PE2-GigabitEthernet2/1/1] quit
```
将接口 GigabitEthernet2/1/2 与 VPN 实例 b 进行关联，配置 IP 地址，并使能 PIM-SM。
```
[PE2] interface gigabitethernet 2/1/2
[PE2-GigabitEthernet2/1/2] ip binding vpn-instance b
[PE2-GigabitEthernet2/1/2] ip address 10.110.3.1 24
[PE2-GigabitEthernet2/1/2] pim sm
[PE2-GigabitEthernet2/1/2] quit
```
将接口 GigabitEthernet2/1/3 与 VPN 实例 a 进行关联，配置 IP 地址，并使能 PIM-SM。
```
[PE2] interface gigabitethernet 2/1/3
[PE2-GigabitEthernet2/1/3] ip binding vpn-instance a
[PE2-GigabitEthernet2/1/3] ip address 10.110.4.1 24
[PE2-GigabitEthernet2/1/3] pim sm
[PE2-GigabitEthernet2/1/3] quit
```
配置 LoopBack1 接口的 IP 地址，并使能 PIM-SM。
```
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 1.1.1.2 32
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit
```
配置 BGP 协议。
```
[PE2] bgp 100
[PE2-bgp] group vpn-g internal
[PE2-bgp] peer vpn-g connect-interface loopback 1
[PE2-bgp] peer 1.1.1.1 group vpn-g
```

```
[PE2-bgp] peer 1.1.1.3 group vpn-g
[PE2–bgp] ip vpn-instance a
[PE2-bgp-a] address-family ipv4
[PE2-bgp-ipv4-a] import-route rip 2
[PE2-bgp-ipv4-a] import-route direct
[PE2-bgp-ipv4-a] quit
[PE2-bgp-a] quit
[PE2–bgp] ip vpn-instance b
[PE2-bgp-b] address-family ipv4
[PE2-bgp-ipv4-b] import-route rip 3
[PE2-bgp-ipv4-b] import-route direct
[PE2-bgp-ipv4-b] quit
[PE2-bgp-b] quit
[PE2–bgp] address-family vpnv4
[PE2–bgp-vpnv4] peer vpn-g enable
[PE2–bgp-vpnv4] quit
[PE2–bgp] quit
```

配置 OSPF 协议。

```
[PE2] ospf 1
[PE2-ospf-1] area 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 1.1.1.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.255.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置 RIP 协议。

```
[PE2] rip 2 vpn-instance a
[PE2-rip-2] network 10.0.0.0
[PE2-rip-2] import-route bgp
[PE2-rip-2] quit
[PE2] rip 3 vpn-instance b
[PE2-rip-3] network 10.0.0.0
[PE2-rip-3] import-route bgp
[PE2-rip-3] return
```

(3) 配置 PE 3

配置全局 Router ID，并使能公网实例中的 IP 组播路由。

```
<PE3> system-view
[PE3] router id 1.1.1.3
[PE3] multicast routing
[PE3-mrib] quit
```

配置 LSR ID，并全局使能 LDP 能力。

```
[PE3] mpls lsr-id 1.1.1.3
[PE3] mpls ldp
[PE3-ldp] quit
```

创建 VPN 实例 a，并为其配置 RD 和 Route Target。

```
[PE3] ip vpn-instance a
[PE3-vpn-instance-a] route-distinguisher 100:1
[PE3-vpn-instance-a] vpn-target 100:1 export-extcommunity
```

```
[PE3-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE3-vpn-instance-a] quit
```
使能 VPN 实例 a 中的 IP 组播路由。
```
[PE3] multicast routing vpn-instance a
[PE3-mrib-a] quit
```
创建 VPN 实例 a 的 MD，并指定 Default-Group、MD 源接口和 Data-Group 范围。
```
[PE3] multicast-domain vpn-instance a
[PE3-md-a] default-group 239.1.1.1
[PE3-md-a] source loopback 1
[PE3-md-a] data-group 225.2.2.0 28
[PE3-md-a] quit
```
创建 VPN 实例 b，并为其配置 RD 和 Route Target。
```
[PE3] ip vpn-instance b
[PE3-vpn-instance-b] route-distinguisher 200:1
[PE3-vpn-instance-b] vpn-target 200:1 export-extcommunity
[PE3-vpn-instance-b] vpn-target 200:1 import-extcommunity
[PE3-vpn-instance-b] quit
```
使能 VPN 实例 b 中的 IP 组播路由。
```
[PE3] multicast routing vpn-instance b
[PE3-mrib-b] quit
```
创建 VPN 实例 b 的 MD，并指定，并指定 Default-Group、MD 源接口和 Data-Group 范围。
```
[PE3] multicast-domain vpn-instance b
[PE3-md-b] default-group 239.2.2.2
[PE3-md-b] source loopback 1
[PE3-md-b] data-group 225.4.4.0 28
[PE3-md-b] quit
```
在公网接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 PIM-SM、MPLS 能力和 LDP 能力。
```
[PE3] interface gigabitethernet 2/1/1
[PE3-GigabitEthernet2/1/1] ip address 192.168.8.1 24
[PE3-GigabitEthernet2/1/1] pim sm
[PE3-GigabitEthernet2/1/1] mpls enable
[PE3-GigabitEthernet2/1/1] mpls ldp enable
[PE3-GigabitEthernet2/1/1] quit
```
将接口 GigabitEthernet2/1/2 与 VPN 实例 a 进行关联，配置 IP 地址，并使能 PIM-SM。
```
[PE3] interface gigabitethernet 2/1/2
[PE3-GigabitEthernet2/1/2] ip binding vpn-instance a
[PE3-GigabitEthernet2/1/2] ip address 10.110.5.1 24
[PE3-GigabitEthernet2/1/2] pim sm
[PE3-GigabitEthernet2/1/2] quit
```
将接口 GigabitEthernet2/1/3 与 VPN 实例 b 进行关联，配置 IP 地址，并使能 PIM-SM。
```
[PE3] interface gigabitethernet 2/1/3
[PE3-GigabitEthernet2/1/3] ip binding vpn-instance b
[PE3-GigabitEthernet2/1/3] ip address 10.110.6.1 24
[PE3-GigabitEthernet2/1/3] pim sm
[PE3-GigabitEthernet2/1/3] quit
```
配置 LoopBack1 接口的 IP 地址，并使能 PIM-SM。

```
[PE3] interface loopback 1
[PE3-LoopBack1] ip address 1.1.1.3 32
[PE3-LoopBack1] pim sm
[PE3-LoopBack1] quit
```

将接口 LoopBack2 与 VPN 实例 b 进行关联，配置 IP 地址，并使能 PIM-SM。

```
[PE3] interface loopback 2
[PE3-LoopBack2] ip binding vpn-instance b
[PE3-LoopBack2] ip address 33.33.33.33 32
[PE3-LoopBack2] pim sm
[PE3-LoopBack2] quit
```

配置 LoopBack2 接口为 VPN b 的 C-BSR 和 C-RP。

```
[PE3] pim vpn-instance b
[PE3-pim-b] c-bsr 33.33.33.33
[PE3-pim-b] c-rp 33.33.33.33
[PE3-pim-b] quit
```

配置 BGP 协议。

```
[PE3] bgp 100
[PE3-bgp] group vpn-g internal
[PE3-bgp] peer vpn-g connect-interface loopback 1
[PE3-bgp] peer 1.1.1.1 group vpn-g
[PE3-bgp] peer 1.1.1.2 group vpn-g
[PE3–bgp] ip vpn-instance a
[PE3-bgp-a] address-family ipv4
[PE3-bgp-ipv4-a] import-route rip 2
[PE3-bgp-ipv4-a] import-route direct
[PE3-bgp-ipv4-a] quit
[PE3-bgp-a] quit
[PE3–bgp] ip vpn-instance b
[PE3-bgp-b] address-family ipv4
[PE3-bgp-ipv4-b] import-route rip 3
[PE3-bgp-ipv4-b] import-route direct
[PE3-bgp-ipv4-b] quit
[PE3-bgp-b] quit
[PE3–bgp] address-family vpnv4
[PE3–bgp-vpnv4] peer vpn-g enable
[PE3–bgp-vpnv4] quit
[PE3–bgp] quit
```

配置 OSPF 协议。

```
[PE3] ospf 1
[PE3-ospf-1] area 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 1.1.1.3 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.255.255
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

配置 RIP 协议。

```
[PE3] rip 2 vpn-instance a
[PE3-rip-2] network 10.0.0.0
```

```
[PE3-rip-2] import-route bgp
[PE3-rip-2] quit
[PE3] rip 3 vpn-instance b
[PE3-rip-3] network 10.0.0.0
[PE3-rip-3] network 33.0.0.0
[PE3-rip-3] import-route bgp
[PE3-rip-3] return
```

(4) 配置 P

使能公网实例中的 IP 组播路由。

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

配置 LSR ID，并全局使能 LDP 能力。

```
[P] mpls lsr-id 2.2.2.2
[P] mpls ldp
[P-ldp] quit
```

在公网接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 PIM-SM、MPLS 能力和 LDP 能力。

```
[P] interface gigabitethernet 2/1/1
[P-GigabitEthernet2/1/1] ip address 192.168.6.2 24
[P-GigabitEthernet2/1/1] pim sm
[P-GigabitEthernet2/1/1] mpls enable
[P-GigabitEthernet2/1/1] mpls ldp enable
[P-GigabitEthernet2/1/1] quit
```

在公网接口 GigabitEthernet2/1/2 上配置 IP 地址，并使能 PIM-SM、MPLS 能力和 LDP 能力。

```
[P] interface gigabitethernet 2/1/2
[P-GigabitEthernet2/1/2] ip address 192.168.7.2 24
[P-GigabitEthernet2/1/2] pim sm
[P-GigabitEthernet2/1/2] mpls enable
[P-GigabitEthernet2/1/2] mpls ldp enable
[P-GigabitEthernet2/1/2] quit
```

在公网接口 GigabitEthernet2/1/3 上配置 IP 地址，并使能 PIM-SM、MPLS 能力和 LDP 能力。

```
[P] interface gigabitethernet 2/1/3
[P-GigabitEthernet2/1/3] ip address 192.168.8.2 24
[P-GigabitEthernet2/1/3] pim sm
[P-GigabitEthernet2/1/3] mpls enable
[P-GigabitEthernet2/1/3] mpls ldp enable
[P-GigabitEthernet2/1/3] quit
```

配置 LoopBack1 接口的 IP 地址，并使能 PIM-SM。

```
[P] interface loopback 1
[P-LoopBack1] ip address 2.2.2.2 32
[P-LoopBack1] pim sm
[P-LoopBack1] quit
```

配置 LoopBack1 接口为公网实例的 C-BSR 和 C-RP。

```
[P] pim
[P-pim] c-bsr 2.2.2.2
[P-pim] c-rp 2.2.2.2
```

```
[P-pim] quit
```

配置 OSPF 协议。

```
[P] ospf 1
[P-ospf-1] area 0.0.0.0
[P-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[P-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.255.255
```

(5) 配置 CE a1

使能 IP 组播路由。

```
<CEa1> system-view
[CEa1] multicast routing
[CEa1-mrib] quit
```

在接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 PIM-SM。

```
[CEa1] interface gigabitethernet 2/1/1
[CEa1-GigabitEthernet2/1/1] ip address 10.110.7.1 24
[CEa1-GigabitEthernet2/1/1] pim sm
[CEa1-GigabitEthernet2/1/1] quit
```

在接口 GigabitEthernet2/1/2 上配置 IP 地址，并使能 PIM-SM。

```
[CEa1] interface gigabitethernet 2/1/2
[CEa1-GigabitEthernet2/1/2] ip address 10.110.2.2 24
[CEa1-GigabitEthernet2/1/2] pim sm
[CEa1-GigabitEthernet2/1/2] quit
```

配置 RIP 协议。

```
[CEa1] rip 2
[CEa1-rip-2] network 10.0.0.0
```

(6) 配置 CE b1

使能 IP 组播路由。

```
<CEb1> system-view
[CEb1] multicast routing
[CEb1-mrib] quit
```

在接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 PIM-SM。

```
[CEb1] interface gigabitethernet 2/1/1
[CEb1-GigabitEthernet2/1/1] ip address 10.110.8.1 24
[CEb1-GigabitEthernet2/1/1] pim sm
[CEb1-GigabitEthernet2/1/1] quit
```

在接口 GigabitEthernet2/1/2 上配置 IP 地址，并使能 PIM-SM。

```
[CEb1] interface gigabitethernet 2/1/2
[CEb1-GigabitEthernet2/1/2] ip address 10.110.3.2 24
[CEb1-GigabitEthernet2/1/2] pim sm
[CEb1-GigabitEthernet2/1/2] quit
```

配置 RIP 协议。

```
[CEb1] rip 3
[CEb1-rip-3] network 10.0.0.0
```

(7) 配置 CE a2

使能 IP 组播路由。

```
<CEa2> system-view
```

```
[CEa2] multicast routing
[CEa2-mrib] quit
```
在接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 IGMP。
```
[CEa2] interface gigabitethernet 2/1/1
[CEa2-GigabitEthernet2/1/1] ip address 10.110.9.1 24
[CEa2-GigabitEthernet2/1/1] igmp enable
[CEa2-GigabitEthernet2/1/1] quit
```
在接口 GigabitEthernet2/1/2 上配置 IP 地址，并使能 PIM-SM。
```
[CEa2] interface gigabitethernet 2/1/2
[CEa2-GigabitEthernet2/1/2] ip address 10.110.4.2 24
[CEa2-GigabitEthernet2/1/2] pim sm
[CEa2-GigabitEthernet2/1/2] quit
```
在接口 GigabitEthernet2/1/3 上配置 IP 地址，并使能 PIM-SM。
```
[CEa2] interface gigabitethernet 2/1/3
[CEa2-GigabitEthernet2/1/3] ip address 10.110.12.1 24
[CEa2-GigabitEthernet2/1/3] pim sm
[CEa2-GigabitEthernet2/1/3] quit
```
配置 LoopBack1 接口的 IP 地址，并使能 PIM-SM。
```
[CEa2] interface loopback 1
[CEa2-LoopBack1] ip address 22.22.22.22 32
[CEa2-LoopBack1] pim sm
[CEa2-LoopBack1] quit
```
配置 LoopBack1 接口为 VPN a 的 BSR 和 RP。
```
[CEa2] pim
[CEa2-pim] c-bsr 22.22.22.22
[CEa2-pim] c-rp 22.22.22.22
[CEa2-pim] quit
```
配置 RIP 协议。
```
[CEa2] rip 2
[CEa2-rip-2] network 10.0.0.0
[CEa2-rip-2] network 22.0.0.0
```
(8) 配置 CE a3

使能 IP 组播路由。
```
<CEa3> system-view
[CEa3] multicast routing
[CEa3-mrib] quit
```
在接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 IGMP。
```
[CEa3] interface gigabitethernet 2/1/1
[CEa3-GigabitEthernet2/1/1] ip address 10.110.10.1 24
[CEa3-GigabitEthernet2/1/1] igmp enable
[CEa3-GigabitEthernet2/1/1] quit
```
在接口 GigabitEthernet2/1/2 上配置 IP 地址，并使能 PIM-SM。
```
[CEa3] interface gigabitethernet 2/1/2
[CEa3-GigabitEthernet2/1/2] ip address 10.110.5.2 24
[CEa3-GigabitEthernet2/1/2] pim sm
[CEa3-GigabitEthernet2/1/2] quit
```

在接口 GigabitEthernet2/1/3 上配置 IP 地址，并使能 PIM-SM。

```
[CEa3] interface gigabitethernet 2/1/3
[CEa3-GigabitEthernet2/1/3] ip address 10.110.12.2 24
[CEa3-GigabitEthernet2/1/3] pim sm
[CEa3-GigabitEthernet2/1/3] quit
```

配置 RIP 协议。

```
[CEa3] rip 2
[CEa3-rip-2] network 10.0.0.0
```

(9) 配置 CE b2

使能 IP 组播路由。

```
<CEb2> system-view
[CEb2] multicast routing
[CEb2-mrib] quit
```

在接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 IGMP。

```
[CEb2] interface gigabitethernet 2/1/1
[CEb2-GigabitEthernet2/1/1] ip address 10.110.11.1 24
[CEb2-GigabitEthernet2/1/1] igmp enable
[CEb2-GigabitEthernet2/1/1] quit
```

在接口 GigabitEthernet2/1/2 上配置 IP 地址，并使能 PIM-SM。

```
[CEb2] interface gigabitethernet 2/1/2
[CEb2-GigabitEthernet2/1/2] ip address 10.110.6.2 24
[CEb2-GigabitEthernet2/1/2] pim sm
[CEb2-GigabitEthernet2/1/2] quit
```

配置 RIP 协议。

```
[CEb2] rip 3
[CEb2-rip-3] network 10.0.0.0
```

4. 验证配置

通过使用 **display multicast-domain default-group** 命令可以查看 Default-Group 的信息。

查看 PE 1 上所有 VPN 实例中 Default-Group 的信息。

```
[PE1] display multicast-domain default-group
 Group address    Source address   Interface     VPN instance
 239.1.1.1        1.1.1.1          MTunnel0      a
```

查看 PE 2 上所有 VPN 实例中 Default-Group 的信息。

```
[PE2] display multicast-domain default-group
 Group address    Source address   Interface     VPN instance
 239.1.1.1        1.1.1.2          MTunnel0      a
 239.1.1.1        1.1.1.2          MTunnel1      b
```

查看 PE 3 上所有 VPN 实例中 Default-Group 的信息。

```
[PE3] display multicast-domain default-group
 Group address    Source address   Interface     VPN instance
 239.1.1.1        1.1.1.3          MTunnel0      a
 239.2.2.2        1.1.1.3          MTunnel1      b
```

1.7.2 跨AS的MD VPN配置举例

1. 组网需求

组网需求如 表 1-13 所示。

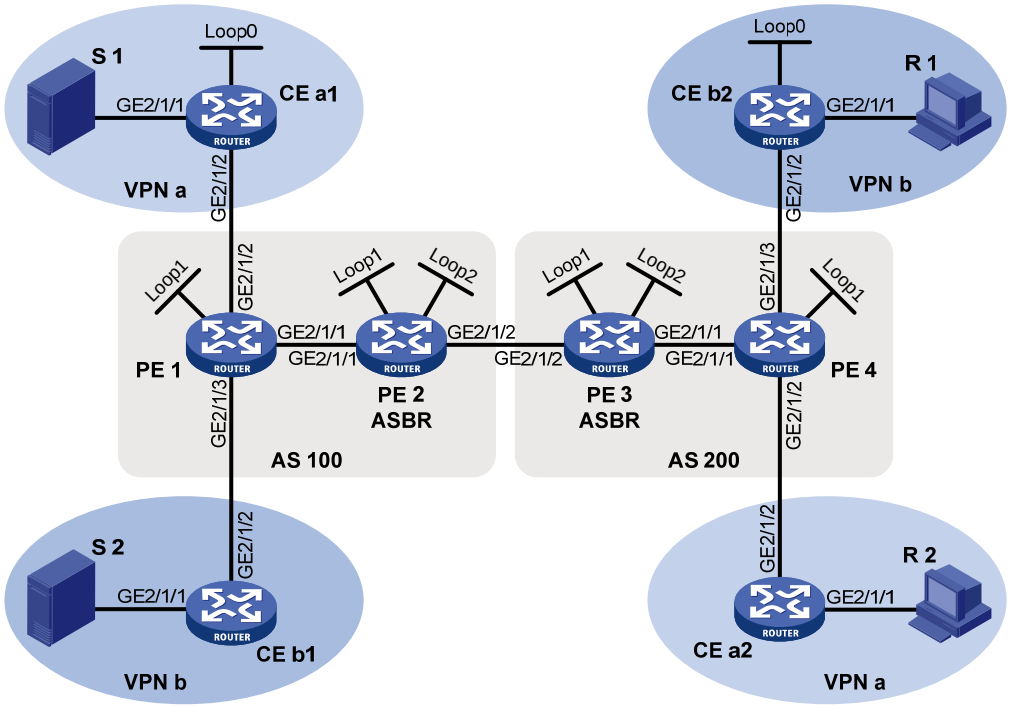
表1-13 跨 AS 的 MD VPN 配置组网需求

项目	组网需求
组播源和接收者	• VPN a 的组播源为 S 1，接收者为 R 2 • VPN b 的组播源为 S 2，接收者为 R 1 • VPN a 中的 Default-Group 为 239.1.1.1，Data-Group 范围为 225.1.1.0～225.1.1.15 • VPN b 中的 Default-Group 为 239.4.4.4，Data-Group 范围为 225.4.4.0～225.4.4.15
PE上各接口所属的VPN实例	• PE 1：GigabitEthernet2/1/2 属于 VPN 实例 a，GigabitEthernet2/1/3 属于 VPN 实例 b，GigabitEthernet2/1/1 和 LoopBack1 属于公网实例 • PE 2：GigabitEthernet2/1/1、GigabitEthernet2/1/2、LoopBack1 和 LoopBack2 属于公网实例 • PE 3：GigabitEthernet2/1/1、GigabitEthernet2/1/2、LoopBack1 和 LoopBack2 属于公网实例 • PE 4：GigabitEthernet2/1/2 属于 VPN 实例 a，GigabitEthernet2/1/3 属于 VPN 实例 b，GigabitEthernet2/1/1 和 LoopBack1 属于公网实例
单播路由协议和MPLS	• 在 AS 100 和 AS 200 中分别配置 OSPF，在各 PE 与 CE 之间也配置 OSPF • 在 PE 1、PE 2、PE 3 和 PE 4 各自的 LoopBack1 接口之间建立 BGP 对等体连接并传递所有私网路由 • 在 AS 100 和 AS 200 中分别配置 MPLS
IP组播路由功能	• 在 PE 1、PE 2、PE 3 和 PE 4 的公网实例中均使能 IP 组播路由 • 在 PE 1 和 PE 4 的 VPN 实例 a 中均使能 IP 组播路由 • 在 PE 1 和 PE 4 的 VPN 实例 b 中均使能 IP 组播路由 • 在 CE a1、CE a2、CE b1、CE b2 上均使能 IP 组播路由
IGMP功能	• 在 CE a2 的 GigabitEthernet2/1/1 接口上使能 IGMPv2 • 在 CE b2 的 GigabitEthernet2/1/1 接口上使能 IGMPv2
PIM功能	• 在 PE 2 和 PE 3 的所有公网接口上均使能 PIM-SM • 在 PE 1 和 PE 4 的所有公网和私网接口上均使能 PIM-SM • 在 CE a1、CE a2、CE b1 和 CE b2 的所有不连接接收者的接口上均使能 PIM-SM • PE 2 和 PE 3 的 LoopBack2 接口为各自所在 AS 的 C-BSR 和 C-RP（服务于所有组播组） • CE a1 的 LoopBack0 接口为 VPN a 的 C-BSR 和 C-RP（服务于所有组播组） • CE b1 的 LoopBack0 接口为 VPN b 的 C-BSR 和 C-RP（服务于所有组播组）

项目	组网需求
MSDP功能	• 在 PE 2 和 PE 3 的 Loopback1 接口之间建立 MSDP 对等体

2. 组网图

图1-12 跨 AS 的 MD VPN 配置组网图



设备	接口	IP地址	设备	接口	IP地址
S 1	-	10.11.5.2/24	R 1	-	10.11.8.2/24
S 2	-	10.11.6.2/24	R 2	-	10.11.7.2/24
PE 1	GE2/1/1	10.10.1.1/24	PE 3	GE2/1/1	10.10.2.1/24
	GE2/1/2	10.11.1.1/24		GE2/1/2	192.168.1.2/24
	GE2/1/3	10.11.2.1/24		Loop1	1.1.1.3/32
	Loop1	1.1.1.1/32		Loop2	22.22.22.22/32
PE 2	GE2/1/1	10.10.1.2/24	PE 4	GE2/1/1	10.10.2.2/24
	GE2/1/2	192.168.1.1/24		GE2/1/2	10.11.3.1/24
	Loop1	1.1.1.2/32		GE2/1/3	10.11.4.1/32
	Loop2	11.11.11.11/32		Loop2	1.1.1.4/32
CE a1	GE2/1/1	10.11.5.1/24	CE b1	GE2/1/1	10.11.6.1/24
	GE2/1/2	10.11.1.2/24		GE2/1/2	10.11.2.2/24
	Loop0	2.2.2.2/32	CE b2	GE2/1/1	10.11.8.1/24
CE a2	GE2/1/1	10.11.7.1/24		GE2/1/2	10.11.4.2/24
	GE2/1/2	10.11.3.2/24		Loop0	3.3.3.3/32

3. 配置步骤

(1) 配置 PE 1

配置全局 Router ID，并使能公网实例中的 IP 组播路由。

```
<PE1> system-view
[PE1] router id 1.1.1.1
[PE1] multicast routing
```

```
[PE1-mrib] quit
```
配置 LSR ID，并全局使能 LDP 能力。
```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls ldp
[PE1-ldp] quit
```
创建 VPN 实例 a，并为其配置 RD 和 Route Target。
```
[PE1] ip vpn-instance a
[PE1-vpn-instance-a] route-distinguisher 100:1
[PE1-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE1-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE1-vpn-instance-a] quit
```
使能 VPN 实例 a 中的 IP 组播路由。
```
[PE1] multicast routing vpn-instance a
[PE1-mrib-a] quit
```
创建 VPN 实例 a 的 MD，并指定 Default-Group、MD 源接口和 Data-Group 范围。
```
[PE1] multicast-domain vpn-instance a
[PE1-md-a] default-group 239.1.1.1
[PE1-md-a] source loopback 1
[PE1-md-a] data-group 225.1.1.0 28
[PE1-md-a] quit
```
创建 VPN 实例 b，并为其配置 RD 和 Route Target。
```
[PE1] ip vpn-instance b
[PE1-vpn-instance-b] route-distinguisher 200:1
[PE1-vpn-instance-b] vpn-target 200:1 export-extcommunity
[PE1-vpn-instance-b] vpn-target 200:1 import-extcommunity
[PE1-vpn-instance-b] quit
```
使能 VPN 实例 b 中的 IP 组播路由。
```
[PE1] multicast routing vpn-instance b
[PE1-mrib-b] quit
```
创建 VPN 实例 b 的 MD，并指定 Default-Group、MD 源接口和 Data-Group 范围。
```
[PE1] multicast-domain vpn-instance b
[PE1-md-b] default-group 239.4.4.4
[PE1-md-b] source loopback 1
[PE1-md-b] data-group 225.4.4.0 28
[PE1-md-b] quit
```
在公网接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 PIM-SM、MPLS 能力和 LDP 能力。
```
[PE1] interface gigabitethernet 2/1/1
[PE1-GigabitEthernet2/1/1] ip address 10.10.1.1 24
[PE1-GigabitEthernet2/1/1] pim sm
[PE1-GigabitEthernet2/1/1] mpls enable
[PE1-GigabitEthernet2/1/1] mpls ldp enable
[PE1-GigabitEthernet2/1/1] quit
```
将接口 GigabitEthernet2/1/2 与 VPN 实例 a 进行关联，配置 IP 地址，并使能 PIM-SM。
```
[PE1] interface gigabitethernet 2/1/2
[PE1-GigabitEthernet2/1/2] ip binding vpn-instance a
[PE1-GigabitEthernet2/1/2] ip address 10.11.1.1 24
```

```
[PE1-GigabitEthernet2/1/2] pim sm
[PE1-GigabitEthernet2/1/2] quit
```
将接口 GigabitEthernet2/1/3 与 VPN 实例 b 进行关联，配置 IP 地址，并使能 PIM-SM。
```
[PE1] interface gigabitethernet 2/1/3
[PE1-GigabitEthernet2/1/3] ip binding vpn-instance b
[PE1-GigabitEthernet2/1/3] ip address 10.11.2.1 24
[PE1-GigabitEthernet2/1/3] pim sm
[PE1-GigabitEthernet2/1/3] quit
```
配置 LoopBack1 接口的 IP 地址，并使能 PIM-SM。
```
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 1.1.1.1 32
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```
配置 BGP 协议。
```
[PE1] bgp 100
[PE1-bgp] group pe1-pe2 internal
[PE1-bgp] peer pe1-pe2 connect-interface loopback 1
[PE1-bgp] peer 1.1.1.2 group pe1-pe2
[PE1-bgp] group pe1-pe4 external
[PE1-bgp] peer pe1-pe4 as-number 200
[PE1-bgp] peer pe1-pe4 ebgp-max-hop 255
[PE1-bgp] peer pe1-pe4 connect-interface loopback 1
[PE1-bgp] peer 1.1.1.4 group pe1-pe4
[PE1–bgp] ip vpn-instance a
[PE1-bgp-a] address-family ipv4
[PE1-bgp-ipv4-a] import-route ospf 2
[PE1-bgp-ipv4-a] import-route direct
[PE1-bgp-ipv4-a] quit
[PE1-bgp-a] quit
[PE1–bgp] ip vpn-instance b
[PE1-bgp-b] address-family ipv4
[PE1-bgp-ipv4-b] import-route ospf 3
[PE1-bgp-ipv4-b] import-route direct
[PE1-bgp-ipv4-b] quit
[PE1-bgp-b] quit
[PE1–bgp] address-family ipv4
[PE1-bgp-ipv4] peer pe1-pe2 enable
[PE1-bgp-ipv4] peer pe1-pe2 label-route-capability
[PE1-bgp-ipv4] quit
[PE1–bgp] address-family vpnv4
[PE1–bgp-vpnv4] peer pe1-pe4 enable
[PE1–bgp-vpnv4] quit
[PE1–bgp] quit
```
配置 OSPF 协议。
```
[PE1] ospf 1
[PE1-ospf-1] area 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
```

```
[PE1-ospf-1-area-0.0.0.0] network 10.10.0.0 0.0.255.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
[PE1] ospf 2 vpn-instance a
[PE1-ospf-2] import-route bgp
[PE1-ospf-2] area 0.0.0.0
[PE1-ospf-2-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[PE1-ospf-2-area-0.0.0.0] quit
[PE1-ospf-2] quit
[PE1] ospf 3 vpn-instance b
[PE1-ospf-3] import-route bgp
[PE1-ospf-3] area 0.0.0.0
[PE1-ospf-3-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[PE1-ospf-3-area-0.0.0.0] quit
[PE1-ospf-3] quit
```

(2) 配置 PE 2

配置全局 Router ID，并使能公网实例中的 IP 组播路由。

```
<PE2> system-view
[PE2] router id 1.1.1.2
[PE2] multicast routing
[PE2-mrib] quit
```

配置 LSR ID，并全局使能 LDP 能力。

```
[PE2] mpls lsr-id 1.1.1.2
[PE2] mpls ldp
[PE2-ldp] quit
```

在公网接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 PIM-SM、MPLS 能力和 LDP 能力。

```
[PE2] interface gigabitethernet 2/1/1
[PE2-GigabitEthernet2/1/1] ip address 10.10.1.2 24
[PE2-GigabitEthernet2/1/1] pim sm
[PE2-GigabitEthernet2/1/1] mpls enable
[PE2-GigabitEthernet2/1/1] mpls ldp enable
[PE2-GigabitEthernet2/1/1] quit
```

在公网接口 GigabitEthernet2/1/2 上配置 IP 地址，并使能 PIM-SM 和 MPLS 能力。

```
[PE2] interface gigabitethernet 2/1/2
[PE2-GigabitEthernet2/1/2] ip address 192.168.1.1 24
[PE2-GigabitEthernet2/1/2] pim sm
[PE2-GigabitEthernet2/1/2] mpls enable
[PE2-GigabitEthernet2/1/2] quit
```

配置 LoopBack1 接口的 IP 地址，并使能 PIM-SM。

```
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 1.1.1.2 32
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit
```

配置 LoopBack2 接口的 IP 地址，并使能 PIM-SM。

```
[PE2] interface loopback 2
[PE2-LoopBack2] ip address 11.11.11.11 32
[PE2-LoopBack2] pim sm
```

```
[PE2-LoopBack2] quit
```
配置 LoopBack2 接口为公网实例的 C-BSR 和 C-RP。
```
[PE2] pim
[PE2-pim] c-bsr 11.11.11.11
[PE2-pim] c-rp 11.11.11.11
[PE2-pim] quit
```
配置 BSR 的服务边界。
```
[PE2] interface gigabitethernet 2/1/2
[PE2-GigabitEthernet2/1/2] pim bsr-boundary
[PE2-GigabitEthernet2/1/2] quit
```
配置 MSDP 对等体。
```
[PE2] msdp
[PE2-msdp] encap-data-enable
[PE2-msdp] peer 1.1.1.3 connect-interface loopback 1
```
配置静态路由。
```
[PE2] ip route-static 1.1.1.3 32 gigabitethernet 2/1/2 192.168.1.2
```
配置 BGP 协议。
```
[PE2] bgp 100
[PE2-bgp] group pe2-pe1 internal
[PE2-bgp] peer pe2-pe1 connect-interface loopback 1
[PE2-bgp] peer 1.1.1.1 group pe2-pe1
[PE2-bgp] group pe2-pe3 external
[PE2-bgp] peer pe2-pe3 as-number 200
[PE2-bgp] peer pe2-pe3 connect-interface loopback 1
[PE2-bgp] peer 1.1.1.3 group pe2-pe3
[PE2-bgp] address-family ipv4
[PE2-bgp-ipv4] peer pe2-pe1 enable
[PE2-bgp-ipv4] peer pe2-pe1 route-policy map2 export
[PE2-bgp-ipv4] peer pe2-pe1 label-route-capability
[PE2-bgp-ipv4] peer pe2-pe3 enable
[PE2-bgp-ipv4] peer pe2-pe3 route-policy map1 export
[PE2-bgp-ipv4] peer pe2-pe3 label-route-capability
[PE2-bgp-ipv4] import-route ospf 1
[PE2-bgp-ipv4] quit
[PE2–bgp] quit
```
配置 OSPF 协议。
```
[PE2] ospf 1
[PE2-ospf-1] area 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 1.1.1.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 11.11.11.11 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 10.10.0.0 0.0.255.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```
配置路由策略。
```
[PE2] route-policy map1 permit node 10
[PE2-route-policy-map1-10] apply mpls-label
[PE2-route-policy-map1-10] quit
```

```
[PE2] route-policy map2 permit node 10
[PE2-route-policy-map2-10] if-match mpls-label
[PE2-route-policy-map2-10] apply mpls-label
[PE2-route-policy-map2-10] quit
```

(3) 配置 PE 3

配置全局 Router ID，并使能公网实例中的 IP 组播路由。

```
<PE3> system-view
[PE3] router id 1.1.1.3
[PE3] multicast routing
[PE3-mrib] quit
```

配置 LSR ID，并全局使能 LDP 能力。

```
[PE3] mpls lsr-id 1.1.1.3
[PE3] mpls ldp
[PE3-ldp] quit
```

在公网接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 PIM-SM、MPLS 能力和 LDP 能力。

```
[PE3] interface gigabitethernet 2/1/1
[PE3-GigabitEthernet2/1/1] ip address 10.10.2.1 24
[PE3-GigabitEthernet2/1/1] pim sm
[PE3-GigabitEthernet2/1/1] mpls enable
[PE3-GigabitEthernet2/1/1] mpls ldp enable
[PE3-GigabitEthernet2/1/1] quit
```

在公网接口 GigabitEthernet2/1/2 上配置 IP 地址，并使能 PIM-SM 和 MPLS 能力。

```
[PE3] interface gigabitethernet 2/1/2
[PE3-GigabitEthernet2/1/2] ip address 192.168.1.2 24
[PE3-GigabitEthernet2/1/2] pim sm
[PE3-GigabitEthernet2/1/2] mpls enable
[PE3-GigabitEthernet2/1/2] quit
```

配置 LoopBack1 接口的 IP 地址，并使能 PIM-SM。

```
[PE3] interface loopback 1
[PE3-LoopBack1] ip address 1.1.1.3 32
[PE3-LoopBack1] pim sm
[PE3-LoopBack1] quit
```

配置 LoopBack2 接口的 IP 地址，并使能 PIM-SM。

```
[PE3] interface loopback 2
[PE3-LoopBack2] ip address 22.22.22.22 32
[PE3-LoopBack2] pim sm
[PE3-LoopBack2] quit
```

配置 LoopBack2 接口为公网实例的 C-BSR 和 C-RP。

```
[PE3] pim
[PE3-pim] c-bsr 22.22.22.22
[PE3-pim] c-rp 22.22.22.22
[PE3-pim] quit
```

配置 BSR 的服务边界。

```
[PE3] interface gigabitethernet 2/1/2
[PE3-GigabitEthernet2/1/2] pim bsr-boundary
[PE3-GigabitEthernet2/1/2] quit
```

配置 MSDP 对等体。

```
[PE3] msdp
[PE3-msdp] encap-data-enable
[PE3-msdp] peer 1.1.1.2 connect-interface loopback 1
```

配置静态路由。

```
[PE3] ip route-static 1.1.1.2 32 gigabitethernet 2/1/2 192.168.1.1
```

配置 BGP 协议。

```
[PE3] bgp 200
[PE3-bgp] group pe3-pe4 internal
[PE3-bgp] peer pe3-pe4 connect-interface loopback 1
[PE3-bgp] peer 1.1.1.4 group pe3-pe4
[PE3-bgp] group pe3-pe2 external
[PE3-bgp] peer pe3-pe2 as-number 100
[PE3-bgp] peer pe3-pe2 connect-interface loopback 1
[PE3-bgp] peer 1.1.1.2 group pe3-pe2
[PE3-bgp] address-family ipv4
[PE3-bgp-ipv4] peer pe3-pe4 enable
[PE3-bgp-ipv4] peer pe3-pe4 route-policy map2 export
[PE3-bgp-ipv4] peer pe3-pe4 label-route-capability
[PE3-bgp-ipv4] peer pe3-pe2 enable
[PE3-bgp-ipv4] peer pe3-pe2 route-policy map1 export
[PE3-bgp-ipv4] peer pe3-pe2 label-route-capability
[PE3-bgp-ipv4] import-route ospf 1
[PE3-bgp-ipv4] quit
[PE3–bgp] quit
```

配置 OSPF 协议。

```
[PE3] ospf 1
[PE3-ospf-1] area 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 1.1.1.3 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 22.22.22.22 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 10.10.0.0 0.0.255.255
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

配置路由策略。

```
[PE3] route-policy map1 permit node 10
[PE3-route-policy-map1-10] apply mpls-label
[PE3-route-policy-map1-10] quit
[PE3] route-policy map2 permit node 10
[PE3-route-policy-map2-10] if-match mpls-label
[PE3-route-policy-map2-10] apply mpls-label
[PE3-route-policy-map2-10] quit
```

(4) 配置 PE 4

配置全局 Router ID，并使能公网实例中的 IP 组播路由。

```
<PE4> system-view
[PE4] router id 1.1.1.4
[PE4] multicast routing
[PE4-mrib] quit
```

配置 LSR ID，并全局使能 LDP 能力。

```
[PE4] mpls lsr-id 1.1.1.4
[PE4] mpls ldp
[PE4-ldp] quit
```

创建 VPN 实例 a，并为其配置 RD 和 Route Target。

```
[PE4] ip vpn-instance a
[PE4-vpn-instance-a] route-distinguisher 100:1
[PE4-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE4-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE4-vpn-instance-a] quit
```

使能 VPN 实例 a 中的 IP 组播路由。

```
[PE4] multicast routing vpn-instance a
[PE4-mrib-a] quit
```

创建 VPN 实例 a 的 MD，并指定 Default-Group、MD 源接口和 Data-Group 范围。

```
[PE4] multicast-domain vpn-instance a
[PE4-md-a] default-group 239.1.1.1
[PE4-md-a] source loopback 1
[PE4-md-a] data-group 225.1.1.0 28
[PE4-md-a] quit
```

创建 VPN 实例 b，并为其配置 RD 和 Route Target。

```
[PE4] ip vpn-instance b
[PE4-vpn-instance-b] route-distinguisher 200:1
[PE4-vpn-instance-b] vpn-target 200:1 export-extcommunity
[PE4-vpn-instance-b] vpn-target 200:1 import-extcommunity
[PE4-vpn-instance-b] quit
```

使能 VPN 实例 b 中的 IP 组播路由。

```
[PE4] multicast routing vpn-instance b
[PE4-mrib-b] quit
```

创建 VPN 实例 b 的 MD，并指定 Default-Group、MD 源接口和 Data-Group 范围。

```
[PE4] multicast-domain vpn-instance b
[PE4-md-b] default-group 239.4.4.4
[PE4-md-b] source loopback 1
[PE4-md-b] data-group 225.4.4.0 28
[PE4-md-b] quit
```

在公网接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 PIM-SM、MPLS 能力和 LDP 能力。

```
[PE4] interface gigabitethernet 2/1/1
[PE4-GigabitEthernet2/1/1] ip address 10.10.2.2 24
[PE4-GigabitEthernet2/1/1] pim sm
[PE4-GigabitEthernet2/1/1] mpls enable
[PE4-GigabitEthernet2/1/1] mpls ldp enable
[PE4-GigabitEthernet2/1/1] quit
```

将接口 GigabitEthernet2/1/2 与 VPN 实例 a 进行关联，配置 IP 地址，并使能 PIM-SM。

```
[PE4] interface gigabitethernet 2/1/2
[PE4-GigabitEthernet2/1/2] ip binding vpn-instance a
[PE4-GigabitEthernet2/1/2] ip address 10.11.3.1 24
[PE4-GigabitEthernet2/1/2] pim sm
```

```
[PE4-GigabitEthernet2/1/2] quit
```
将接口 GigabitEthernet2/1/3 与 VPN 实例 b 进行关联，配置 IP 地址，并使能 PIM-SM。
```
[PE4] interface gigabitethernet 2/1/3
[PE4-GigabitEthernet2/1/3] ip binding vpn-instance b
[PE4-GigabitEthernet2/1/3] ip address 10.11.4.1 24
[PE4-GigabitEthernet2/1/3] pim sm
[PE4-GigabitEthernet2/1/3] quit
```
配置 LoopBack1 接口的 IP 地址，并使能 PIM-SM。
```
[PE4] interface loopback 1
[PE4-LoopBack1] ip address 1.1.1.4 32
[PE4-LoopBack1] pim sm
[PE4-LoopBack1] quit
```
配置 BGP 协议。
```
[PE4] bgp 200
[PE4-bgp] group pe4-pe3 internal
[PE4-bgp] peer pe4-pe3 connect-interface loopback 1
[PE4-bgp] peer 1.1.1.3 group pe4-pe3
[PE4-bgp] group pe4-pe1 external
[PE4-bgp] peer pe4-pe1 as-number 100
[PE4-bgp] peer pe4-pe1 ebgp-max-hop 255
[PE4-bgp] peer pe4-pe1 connect-interface loopback 1
[PE4-bgp] peer 1.1.1.1 group pe4-pe1
[PE4–bgp] ip vpn-instance a
[PE4-bgp-a] address-family ipv4
[PE4-bgp-ipv4-a] import-route ospf 2
[PE4-bgp-ipv4-a] import-route direct
[PE4-bgp-ipv4-a] quit
[PE4-bgp-a] quit
[PE4–bgp] ip vpn-instance b
[PE4-bgp-b] address-family ipv4
[PE4-bgp-ipv4-b] import-route ospf 3
[PE4-bgp-ipv4-b] import-route direct
[PE4-bgp-ipv4-b] quit
[PE4-bgp-b] quit
[PE4–bgp] address-family ipv4
[PE4-bgp-ipv4] peer pe4-pe3 enable
[PE4-bgp-ipv4] peer pe4-pe3 label-route-capability
[PE4-bgp-ipv4] quit
[PE4–bgp] address-family vpnv4
[PE4–bgp-vpnv4] peer pe4-pe1 enable
[PE4–bgp-vpnv4] quit
[PE4–bgp] quit
```
配置 OSPF 协议。
```
[PE4] ospf 1
[PE4-ospf-1] area 0.0.0.0
[PE4-ospf-1-area-0.0.0.0] network 1.1.1.4 0.0.0.0
[PE4-ospf-1-area-0.0.0.0] network 10.10.0.0 0.0.255.255
```

```
[PE4-ospf-1-area-0.0.0.0] quit
[PE4-ospf-1] quit
[PE4] ospf 2 vpn-instance a
[PE4-ospf-2] import-route bgp
[PE4-ospf-2] area 0.0.0.0
[PE4-ospf-2-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[PE4-ospf-2-area-0.0.0.0] quit
[PE4-ospf-2] quit
[PE4] ospf 3 vpn-instance b
[PE4-ospf-3] import-route bgp
[PE4-ospf-3] area 0.0.0.0
[PE4-ospf-3-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[PE4-ospf-3-area-0.0.0.0] quit
[PE4-ospf-3] quit
```

(5) 配置 CE a1

使能 IP 组播路由。

```
<CEa1> system-view
[CEa1] multicast routing
[CEa1-mrib] quit
```

在接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 PIM-SM。

```
[CEa1] interface gigabitethernet 2/1/1
[CEa1-GigabitEthernet2/1/1] ip address 10.11.5.1 24
[CEa1-GigabitEthernet2/1/1] pim sm
[CEa1-GigabitEthernet2/1/1] quit
```

在接口 GigabitEthernet2/1/2 上配置 IP 地址，并使能 PIM-SM。

```
[CEa1] interface gigabitethernet 2/1/2
[CEa1-GigabitEthernet2/1/2] ip address 10.11.1.2 24
[CEa1-GigabitEthernet2/1/2] pim sm
[CEa1-GigabitEthernet2/1/2] quit
```

配置 LoopBack1 接口的 IP 地址，并使能 PIM-SM。

```
[CEa1] interface loopback 1
[CEa1-LoopBack1] ip address 2.2.2.2 32
[CEa1-LoopBack1] pim sm
[CEa1-LoopBack1] quit
```

配置 LoopBack1 接口为 VPN a 的 C-BSR 和 C-RP。

```
[CEa1] pim
[CEa1-pim] c-bsr 2.2.2.2
[CEa1-pim] c-rp 2.2.2.2
[CEa1-pim] quit
```

配置 OSPF 协议。

```
[CEa1] ospf 1
[CEa1-ospf-1] area 0.0.0.0
[CEa1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[CEa1-ospf-1-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[CEa1-ospf-1-area-0.0.0.0] quit
[CEa1-ospf-1] quit
```

(6) 配置 CE b1

使能 IP 组播路由。

```
<CEb1> system-view
[CEb1] multicast routing
[CEb1-mrib] quit
```

在接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 PIM-SM。

```
[CEb1] interface gigabitethernet 2/1/1
[CEb1-GigabitEthernet2/1/1] ip address 10.11.6.1 24
[CEb1-GigabitEthernet2/1/1] pim sm
[CEb1-GigabitEthernet2/1/1] quit
```

在接口 GigabitEthernet2/1/2 上配置 IP 地址，并使能 PIM-SM。

```
[CEb1] interface gigabitethernet 2/1/2
[CEb1-GigabitEthernet2/1/2] ip address 10.11.2.2 24
[CEb1-GigabitEthernet2/1/2] pim sm
[CEb1-GigabitEthernet2/1/2] quit
```

配置 OSPF 协议。

```
[CEb1] ospf 1
[CEb1-ospf-1] area 0.0.0.0
[CEb1-ospf-1-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[CEb1-ospf-1-area-0.0.0.0] quit
[CEb1-ospf-1] quit
```

(7) 配置 CE a2

使能 IP 组播路由。

```
<CEa2> system-view
[CEa2] multicast routing
[CEa2-mrib] quit
```

在接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 IGMP。

```
[CEa2] interface gigabitethernet 2/1/1
[CEa2-GigabitEthernet2/1/1] ip address 10.11.7.1 24
[CEa2-GigabitEthernet2/1/1] igmp enable
[CEa2-GigabitEthernet2/1/1] quit
```

在接口 GigabitEthernet2/1/2 上配置 IP 地址，并使能 PIM-SM。

```
[CEa2] interface gigabitethernet 2/1/2
[CEa2-GigabitEthernet2/1/2] ip address 10.11.3.2 24
[CEa2-GigabitEthernet2/1/2] pim sm
[CEa2-GigabitEthernet2/1/2] quit
```

配置 OSPF 协议。

```
[CEa2] ospf 1
[CEa2-ospf-1] area 0.0.0.0
[CEa2-ospf-1-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[CEa2-ospf-1-area-0.0.0.0] quit
[CEa2-ospf-1] quit
```

(8) 配置 CE b2

使能 IP 组播路由。

```
<CEb2> system-view
```

```
[CEb2] multicast routing
[CEb2-mrib] quit
```

在接口 GigabitEthernet2/1/1 上配置 IP 地址，并使能 IGMP。

```
[CEb2] interface gigabitethernet 2/1/1
[CEb2-GigabitEthernet2/1/1] ip address 10.11.8.1 24
[CEb2-GigabitEthernet2/1/1] igmp enable
[CEb2-GigabitEthernet2/1/1] quit
```

在接口 GigabitEthernet2/1/2 上配置 IP 地址，并使能 PIM-SM。

```
[CEb2] interface gigabitethernet 2/1/2
[CEb2-GigabitEthernet2/1/2] ip address 10.11.4.2 24
[CEb2-GigabitEthernet2/1/2] pim sm
[CEb2-GigabitEthernet2/1/2] quit
```

配置 LoopBack1 接口的 IP 地址，并使能 PIM-SM。

```
[CEb2] interface loopback 1
[CEb2-LoopBack1] ip address 3.3.3.3 32
[CEb2-LoopBack1] pim sm
[CEb2-LoopBack1] quit
```

配置 LoopBack1 接口为 VPN b 的 C-BSR 和 C-RP。

```
[CEb2] pim
[CEb2-pim] c-bsr 3.3.3.3
[CEb2-pim] c-rp 3.3.3.3
[CEb2-pim] quit
```

配置 OSPF 协议。

```
[CEb2] ospf 1
[CEb2-ospf-1] area 0.0.0.0
[CEb2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[CEb2-ospf-1-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[CEb2-ospf-1-area-0.0.0.0] quit
[CEb2-ospf-1] quit
```

4. 验证配置

通过使用 **display multicast-domain default-group** 命令可以查看 Default-Group 的信息。

查看 PE 1 上所有 VPN 实例中 Default-Group 的信息。

```
[PE1] display multicast-domain default-group
 Group address    Source address   Interface     VPN instance
 239.1.1.1        1.1.1.1          MTunnel0      a
 239.4.4.4        1.1.1.1          MTunnel1      b
```

查看 PE 4 上所有 VPN 实例中 Default-Group 的信息。

```
[PE4] display multicast-domain default-group
 Group address    Source address   Interface     VPN instance
 239.1.1.1        1.1.1.4          MTunnel0      a
 239.4.4.4        1.1.1.4          MTunnel1      b
```

1.8 常见配置错误举例

1.8.1 无法建立Default-MDT

1. 故障现象

无法正确建立 Default-MDT，不同 PE 上相同的 VPN 实例之间无法建立起 PIM 邻居关系。

2. 分析

- MTI 必须有 Default-Group 和可用的 MD 源接口 IP 地址才能生效，否则无法建立 Default-MDT。
- 在不同的 PE 上，相同的 VPN 实例需要指定相同的 Default-Group，每个 Default-Group 唯一标识一个 Default-MDT。如果不同 PE 上相同的 VPN 实例没有指定相同的 Default-Group，则该 VPN 实例在不同 PE 上无法建立 Default-MDT。
- 在不同的 PE 上，相同 VPN 实例的各接口必须使用相同的 PIM 模式，P 上所有接口必须使用相同的 PIM 模式，这样才能正确地建立 Default-MDT，本地 PE 和远端 PE 相同的 VPN 实例上才能建立 PIM 邻居关系。否则无法建立 Default-MDT。
- 只有配置了 BGP 和单播路由，PIM 才能正确地获取路由信息；只有 VPN 实例中至少一个接口上使能了 PIM 协议，MTI 上的 PIM 协议才会被使能，从而使不同 PE 相同的 VPN 实例之间建立 PIM 邻居。否则无法建立 PIM 邻居关系。

3. 处理过程

(1) 检查 MTI 的接口状态。使用 **display interface** 命令检查 MTI 的接口状态和地址封装信息。

(2) 检查 Default-Group。使用 **display multicast-domain default-group** 命令检查不同 PE 上相同的 VPN 实例是否配置有相同的 Default-Group。

(3) 检查各设备 VPN 实例中是否至少在一个接口上使能了 PIM 协议，不同 PE 属于同一 VPN 实例的各接口上是否使用了相同的 PIM 模式，以及 P 的各接口上是否使用了相同的 PIM 模式。使用 **display pim interface verbose** 命令查看各接口上的 PIM 信息。

(4) 检查单播路由。使用 **display ip routing-table** 命令检查本地 PE 的 VPN 实例是否有到达远端 PE 的相同 VPN 实例的单播路由项。

(5) 检查是否配置 BGP 对等体。使用 **display bgp peer** 命令查看配置的 BGP 对等体信息。

1.8.2 VPN实例无法正确建立组播路由表

1. 故障现象

VPN 实例无法正确建立起组播路由表。

2. 分析

- 如果 VPN 实例使能的是 PIM-SM，需要有该 VPN 实例的 BSR 信息，否则无法正确建立该 VPN 实例的组播路由表。
- 如果 VPN 实例使能的是 PIM-SM，需要有该 VPN 实例的 RP 信息，如果没有通向 RP 的单播路由，公网实例和 VPN 实例没有正确建立 PIM 邻居关系，VPN 实例就无法正确建立组播路由表。
- 私网 DR 需要有到达私网 RP 的路由，私网内要有到达组播源的路由。

3. 处理过程

(1) 使用**display pim bsr-info**命令查看公网实例和VPN实例是否有BSR信息。如果不存在BSR信息，则需要查看是否有通向 BSR 的单播路由。

(2) 使用 **display pim rp-info** 命令查看 RP 信息是否正确。如果没有 RP 信息，则检查是否有通向 RP 的单播路由。使用 **display pim neighbor** 命令查看公网和私网上是否正确建立了邻居关系。

(3) 使用 **ping** 命令检查私网 DR 与私网 RP 之间、接收者与组播源之间是否通达。

目 录

1 MLD Snooping

说明

- 本特性该特性仅在安装了 SIC 4GSW/SIC 4GSWP、HMIM-24GSW/24GSWP、HMIM-8GSW 二层交换卡的款型和 MSR3600-28/MSR 3600-51 的固定二层接口上支持。
- 文中的交换机指的是安装了二层以太网接口模块的路由器。

1.1 MLD Snooping简介

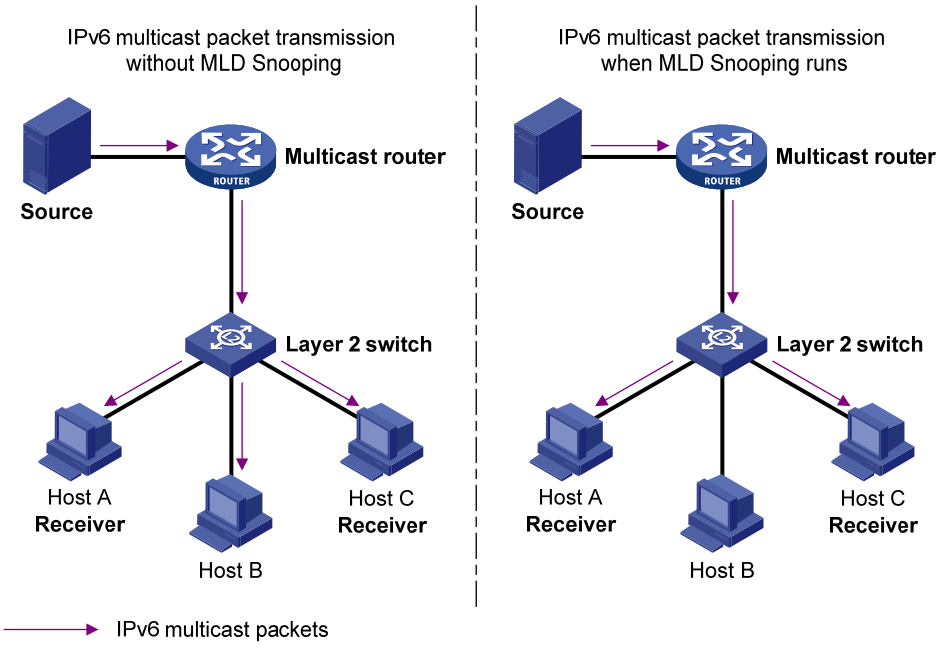
MLD Snooping（Multicast Listener Discovery Snooping，组播侦听者发现协议窥探）运行在二层设备上，通过侦听三层设备与主机之间的 MLD 报文来生成二层组播转发表，从而管理和控制 IPv6 组播数据报文的转发，实现 IPv6 组播数据报文在二层的按需分发。

1.1.1 MLD Snooping原理

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

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

图1-1 二层设备运行 MLD Snooping 前后的对比



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

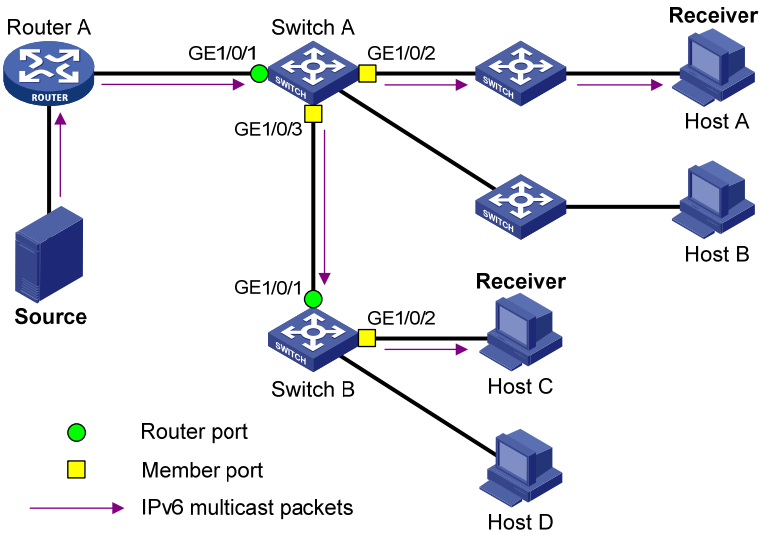
- 减少了二层网络中的广播报文，节约了网络带宽；
- 增强了 IPv6 组播信息的安全性；
- 为实现对每台主机的单独计费带来了方便。

1.1.2 MLD Snooping基本概念

1. MLD Snooping相关端口

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

图1-2 MLD Snooping 相关端口



结合 图 1-2，介绍一下MLD Snooping相关的端口概念：

- 路由器端口（Router Port）：二层设备上朝向三层组播设备（DR 或 MLD 查询器）一侧的端口，如 Switch A 和 Switch B 各自的 GigabitEthernet1/0/1 端口。二层设备将本设备上的所有路由器端口都记录在路由器端口列表中。
- 成员端口（Member Port）：又称 IPv6 组播组成员端口，表示二层设备上朝向 IPv6 组播组成员一侧的端口，如 Switch A 的 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 端口，以及 Switch B 的 GigabitEthernet1/0/2 端口。二层设备将本设备上的所有成员端口都记录在 MLD Snooping 转发表中。

说明

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

---

2. MLD Snooping动态端口老化定时器

表1-1 MLD Snooping 动态端口老化定时器

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

说明

MLD Snooping 端口老化机制只针对动态端口，静态端口永不老化。

1.1.3 MLD Snooping工作机制

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

说明

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

1. 普遍组查询

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

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

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

2. 报告成员关系

以下情况，主机会向 MLD 查询器发送 MLD 成员关系报告报文：

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

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

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

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

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。有关主机上的 MLD 成员关系报告抑制机制的详细介绍，请参见“IP 组播配置指导”中的“MLD”。

---

3. 离开组播组

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

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

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

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

1.1.4 协议规范

与 MLD Snooping 相关的协议规范有：

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

1.2 MLD Snooping配置任务简介

表1-2 MLD Snooping 配置任务简介

配置任务		说明	详细配置
配置MLD Snooping基本功能	使能MLD Snooping	必选	1.3.2
	配置MLD Snooping版本	可选	1.3.3
	配置MLD Snooping转发表项的全局最大数量	可选	1.3.4
配置MLD Snooping端口功能	配置动态端口老化定时器	可选	1.4.2
	配置静态端口	可选	1.4.3
	配置模拟主机加入	可选	1.4.4
	配置端口快速离开	可选	1.4.5
	禁止端口成为动态路由器端口	可选	1.4.6
配置MLD Snooping查询器	使能MLD Snooping查询器	可选	1.5.2
	配置MLD查询和响应	可选	1.5.3
调整MLD报文	配置MLD报文的源IPv6地址	可选	1.6.2
	配置MLD报文的802.1p优先级	可选	1.6.3
配置MLD Snooping策略	配置IPv6组播组过滤器	可选	1.7.2
	配置IPv6组播数据报文源端口过滤	可选	1.7.3
	配置丢弃未知IPv6组播数据报文	可选	1.7.4
	配置MLD成员关系报告报文抑制	可选	1.7.5
	配置端口加入的IPv6组播组最大数量	可选	1.7.6
	配置IPv6组播组替换功能	可选	1.7.7

1.3 配置MLD Snooping基本功能

1.3.1 配置准备

在配置 MLD Snooping 基本功能之前，需完成以下任务：

- 配置相应 VLAN

在配置 MLD Snooping 基本功能之前，需准备以下数据：

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

1.3.2 使能MLD Snooping

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

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

1. 使能指定VLAN内的MLD Snooping

表1-3 在 VLAN 内使能 MLD Snooping

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

2. 在VLAN内使能MLD Snooping

表1-4 在 VLAN 内使能 MLD Snooping

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

1.3.3 配置MLD Snooping版本

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

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

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

1. 配置指定VLAN内的MLD Snooping版本

表1-5 配置指定 VLAN 内的 MLD Snooping 版本

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

2. 在VLAN内配置MLD Snooping版本

表1-6 在 VLAN 内配置 MLD Snooping 版本

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

说明

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

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

有关静态加入的详细配置，请参见“1.4.3 配置静态端口”。

1.3.4 配置MLD Snooping转发表项的全局最大数量

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

表1-7 配置 MLD Snooping 转发表项的全局最大数量

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

说明

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

1.4 配置MLD Snooping端口功能

1.4.1 配置准备

在配置 MLD Snooping 端口功能之前，需完成以下任务：

- 在 VLAN 内使能 MLD Snooping

在配置 MLD Snooping 端口功能之前，需准备以下数据：

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

1.4.2 配置动态端口老化定时器

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

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

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

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

说明

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

1. 全局配置动态端口老化定时器

表1-8 全局配置动态端口老化定时器

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

2. 在VLAN内配置动态端口老化定时器

表1-9 在 VLAN 内配置动态端口老化定时器

操作	命令	说明
进入系统视图	**system-view**	-

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

1.4.3 配置静态端口

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

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

表1-10 配置静态端口

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网	**interface** *interface-type interface-number*	-
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
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

说明

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

1.4.4 配置模拟主机加入

通常情况下，运行 MLD 的主机会对 MLD 查询器发出的查询报文进行响应。如果主机由于某种原因无法响应，就可能导致三层组播设备认为该网段没有该 IPv6 组播组的成员，从而取消相应的转发路径。

为避免这种情况的发生，可以将二层设备的端口配置成为 IPv6 组播组成员（即配置模拟主机加入）。当收到 MLD 查询报文时由模拟主机进行响应，从而保证该二层设备能够继续收到 IPv6 组播报文。

模拟主机加入功能的实现原理如下：

- 在某端口上使能模拟主机加入功能时，该端口会主动发送一个 MLD 成员关系报告报文；

- 在某端口上使能了模拟主机加入功能后，当收到 MLD 普遍组查询报文时，该端口会响应一个 MLD 成员关系报告报文；
- 在某端口上关闭模拟主机加入功能时，该端口会发送一个 MLD 离开组报文。

说明

与静态成员端口不同，配置了模拟主机加入的端口会作为动态成员端口而参与动态成员端口的老化过程。

表1-11 配置模拟主机加入

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

1.4.5 配置端口快速离开

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

对于一个 VLAN 而言，只有当端口下只有一个接收者时，才可使能端口快速离开功能；否则，若端口下有多个接收者，一个接收者的离开将导致属于同一 IPv6 组播组的其它接收者无法收到 IPv6 组播数据。

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

1. 全局配置端口快速离开

表1-12 全局配置端口快速离开

操作	命令	说明
进入系统视图	**system-view**	-
进入MLD-Snooping视图	**mld-snooping**	-
全局使能端口快速离开功能	**fast-leave** [**vlan** *vlan-list*]	缺省情况下，端口快速离开功能处于关闭状态

2. 在端口上配置端口快速离开

表1-13 在端口上配置端口快速离开

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入二层以太网	**interface** *interface-type interface-number*	-
在端口上使能端口快速离开功能	**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

1.4.6 禁止端口成为动态路由器端口

目前，在 IPv6 组播用户接入网络中存在以下问题：

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

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

说明

本配置与静态路由器端口的配置互不影响。

表1-14 禁止端口成为动态路由器端口

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网	**interface** *interface-type interface-number*	-
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，不禁止端口成为动态路由器端口

1.5 配置MLD Snooping查询器

1.5.1 配置准备

在配置 MLD Snooping 查询器之前，需完成以下任务：

- 在 VLAN 内使能 MLD Snooping

在配置 MLD Snooping 查询器之前，需准备以下数据：

- MLD 普遍组查询报文的发送间隔
- MLD 特定组查询报文的发送间隔

- MLD 普遍组查询的最大响应时间

1.5.2 使能MLD Snooping查询器

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

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

提示

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

表1-15 使能 MLD Snooping 查询器

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

1.5.3 配置MLD查询和响应

可以根据网络的实际情况来修改 MLD 普遍组查询报文的发送间隔。

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

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

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

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

提示

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

1. 全局配置MLD查询和响应

表1-16 全局配置 MLD 查询和响应

操作	命令	说明
进入系统视图	**system-view**	-
进入MLD-Snooping视图	**mld-snooping**	-
全局配置MLD普遍组查询的最大响应时间	**max-response-time** *interval*	缺省情况下，MLD普遍组查询的最大响应时间为10秒
全局配置MLD特定组查询报文的发送间隔	**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

2. 在VLAN内配置MLD查询和响应

表1-17 在 VLAN 内配置 MLD 查询和响应

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

1.6 调整MLD报文

1.6.1 配置准备

在调整 MLD 报文之前，需完成以下任务：

- 在 VLAN 内使能 MLD Snooping

在调整 MLD 报文之前，需准备以下数据：

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

- MLD 离开组报文的源 IPv6 地址
- MLD 报文的 802.1p 优先级

1.6.2 配置MLD报文的源IPv6 地址

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

用户也可以通过本配置改变模拟主机或 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。

提示

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。

表1-18 配置 MLD 报文的源 IPv6 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
配置MLD普遍组查询报文的源IPv6地址	**mld-snooping general-query source-ip** *ip-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
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
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
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

1.6.3 配置MLD报文的 802.1p优先级

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 报文的 802.1p 优先级。

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

1. 全局配置MLD报文的 802.1p优先级

表1-19 全局配置 MLD 报文的 802.1p 优先级

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

2. 在VLAN内配置MLD报文的 802.1p优先级

表1-20 在 VLAN 内配置 MLD 报文的 802.1p 优先级

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

1.7 配置MLD Snooping策略

1.7.1 配置准备

在配置 MLD Snooping 策略之前，需完成以下任务：

- 在 VLAN 内使能 MLD Snooping

在配置 MLD Snooping 策略之前，需准备以下数据：

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

1.7.2 配置IPv6 组播组过滤器

提示

本配置只对动态组播组有效，对静态组播组无效。

在使能了 MLD Snooping 的二层设备上，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。

在实际应用中，当用户点播某个组播节目时，主机会发起一个 MLD 成员关系报告报文，该报文到达二层设备后，进行 ACL 检查：如果该接收端口可以加入这个 IPv6 组播组，则将其列入到 MLD Snooping 转发表中；否则二层设备就丢弃该报文。这样，未通过 ACL 检查的 IPv6 组播数据就不会送到该端口，从而达到控制用户点播组播节目的目的。

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

1. 全局配置IPv6 组播组过滤器

表1-21 全局配置 IPv6 组播组过滤器

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

2. 在端口上配置IPv6 组播组过滤器

表1-22 在端口上配置 IPv6 组播组过滤器

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

1.7.3 配置IPv6 组播数据报文源端口过滤

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：

- 使能该功能后，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。

用户既可在 MLD-Snooping 视图下对指定端口进行全局配置，也可在接口视图下只对当前端口进行配置，二者的配置优先级相同。

1. 全局配置IPv6 组播数据报文源端口过滤

表1-23 全局配置 IPv6 组播数据报文源端口过滤

操作	命令	说明
进入系统视图	**system-view**	-
进入MLD-Snooping视图	**mld-snooping**	-
使能指定端口的IPv6组播数据报文源端口过滤功能	**source-deny port** *interface-list*	缺省情况下，端口上的IPv6组播数据报文源端口过滤功能处于关闭状态

2. 在端口上配置IPv6 组播数据报文源端口过滤

表1-24 在端口上配置 IPv6 组播数据报文源端口过滤

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
使能当前端口的IPv6组播数据报文源端口过滤功能	**mld-snooping source-deny**	缺省情况下，端口上的IPv6组播数据报文源端口过滤功能处于关闭状态

说明

该特性仅在安装了 HMIM 24GSW/HMIM 24GSW-POE/HMIM 8GSW 二层交换卡的款型和 MSR3600-28/MSR 3600-51 的固定二层接口上支持。

1.7.4 配置丢弃未知IPv6 组播数据报文

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

- 当使能了丢弃未知 IPv6 组播数据报文功能时，二层设备将丢弃所有收到的未知 IPv6 组播数据报文；
- 当关闭了丢弃未知 IPv6 组播数据报文功能时，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。

用户在 VLAN 内配置丢弃未知 IPv6 组播数据报文。

表1-25 在 VLAN 内配置丢弃未知 IPv6 组播数据报文

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
在VLAN内使能丢弃未知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

说明

对于安装 SIC 4GSW/SIC 4GSWP 二层交换卡的款型，在使能了丢弃未知 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。

1.7.5 配置MLD成员关系报告报文抑制

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

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

表1-26 配置 MLD 成员关系报告报文抑制

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

说明

该特性该特性仅在安装了 HMIM 24GSW/HMIM 24GSW-POE/HMIM 8GSW 二层交换卡的款型和 MSR3600-28/MSR 3600-51 的固定二层接口上支持。

1.7.6 配置端口加入的IPv6 组播组最大数量

提示

本配置只对动态组播组有效，对静态组播组无效。

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

表1-27 配置端口加入的 IPv6 组播组最大数量

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网	**interface** *interface-type interface-number*	-
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，端口加入的IPv6组播组最大数量为4294967295

说明

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

1.7.7 配置IPv6 组播组替换功能

提示

本配置只对动态组播组有效，对静态组播组无效。

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

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

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

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

1. 全局配置IPv6 组播组替换功能

表1-28 全局配置 IPv6 组播组替换功能

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

2. 在端口上配置IPv6 组播组替换功能

表1-29 在端口上配置 IPv6 组播组替换功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网	**interface** *interface-type interface-number*	-

操作	命令	说明
在端口上使能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

1.8 MLD Snooping显示和维护

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

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

表1-30 MLD Snooping 显示和维护

操作	命令
显示IPv6二层组播的IP组播组信息（MSR 2600/MSR 3600）	**display ipv6 l2-multicast ip** [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*]
显示IPv6二层组播的IP组播组信息（MSR 5600）	**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（MSR 2600/MSR 3600）	**display ipv6 l2-multicast ip forwarding** [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*]
显示IPv6二层组播的IP转发表信息（MSR 5600）	**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（MSR 2600/MSR 3600）	**display ipv6 l2-multicast mac** [*mac-address*] [**vlan** *vlan-id*]
显示IPv6二层组播的MAC组播组信息（MSR 5600）	**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（MSR 2600/MSR 3600）	**display ipv6 l2-multicast mac forwarding** [*mac-address*] [**vlan** *vlan-id*]
显示IPv6二层组播的MAC转发表信息（MSR 5600）	**display ipv6 l2-multicast mac forwarding** [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]
显示MLD Snooping的状态信息	**display mld-snooping** [**global** | **vlan** *vlan-id*]
显示IPv6动态组播组的MLD Snooping转发表项信息（MSR 2600/MSR 3600）	**display mld-snooping group** [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**]
显示IPv6动态组播组的MLD Snooping转发表项信息（MSR 5600）	**display mld-snooping group** [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
显示IPv6动态路由器端口的信息（MSR 2600/MSR 3600）	**display mld-snooping router-port** [**vlan** *vlan-id*]
显示IPv6动态路由器端口的信息（MSR 5600）	**display mld-snooping router-port** [**vlan** *vlan-id*] [**slot** *slot-number*]
显示IPv6静态组播组的MLD Snooping转发表项信息（MSR 2600/MSR 3600）	**display mld-snooping static-group** [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**]
显示IPv6静态组播组的MLD Snooping转发表项信息（MSR 5600）	**display mld-snooping static-group** [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

操作	命令
显示IPv6静态路由器端口的信息（MSR 2600/MSR 3600）	**display mld-snooping static-router-port** [**vlan** *vlan-id*]
显示IPv6静态路由器端口的信息（MSR 5600）	**display mld-snooping static-router-port** [**vlan** *vlan-id*] [**slot** *slot-number*]
显示MLD Snooping监听到的MLD报文统计信息	**display mld-snooping statistics**
清除IPv6动态组播组的MLD Snooping转发表项信息	**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报文统计信息	**reset mld-snooping statistics**

1.9 MLD Snooping典型配置举例

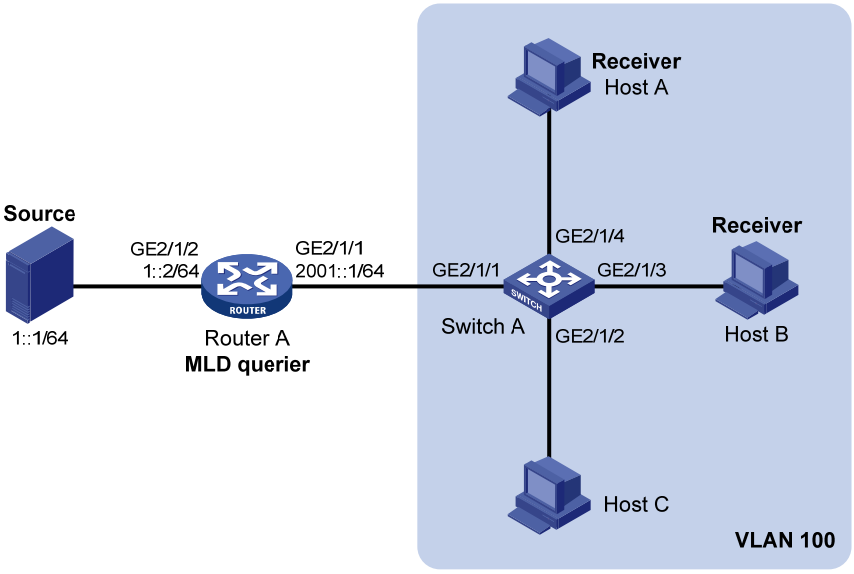
1.9.1 IPv6 组策略及模拟主机加入配置举例

1. 组网需求

- 如 图 1-3 所示，Router A通过GigabitEthernet2/1/2 接口连接IPv6 组播源（Source），通过GigabitEthernet2/1/1 接口连接Switch A；Router A上运行MLDv1，Switch A上运行版本 1 的MLD Snooping，并由Router A充当MLD查询器。
- 通过配置，使 Host A 和 Host B 能且只能接收发往 IPv6 组播组 FF1E::101 的 IPv6 组播数据，并且当 Host A 和 Host B 即使发生意外而临时中断接收 IPv6 组播数据时，发往 IPv6 组播组 FF1E::101 的 IPv6 组播数据也能不间断地通过 Switch A 的接口 GigabitEthernet2/1/3 和 GigabitEthernet2/1/4 转发出去；同时，使 Switch A 将收到的未知 IPv6 组播数据直接丢弃，避免在其所属的 VLAN 100 内广播。

2. 组网图

图1-3 IPv6 组策略及模拟主机加入配置组网图



3. 配置步骤

(1) 配置 IPv6 地址

请按照 图 1-3 配置各接口的IPv6 地址和前缀长度，具体配置过程略。

(2) 配置 Router A

使能 IPv6 组播路由，在接口 GigabitEthernet2/1/2 上使能 IPv6 PIM-DM，并在接口 GigabitEthernet2/1/1 上使能 MLD。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mld enable
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ipv6 pim dm
[RouterA-GigabitEthernet2/1/2] quit
```

(3) 配置 Switch A

全局使能 MLD Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 到 GigabitEthernet2/1/4 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并使能丢弃未知 IPv6 组播数据报文功能。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 2/1/1 to gigabitethernet 2/1/4
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping drop-unknown
```

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

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

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

在 GigabitEthernet2/1/3 和 GigabitEthernet2/1/4 上分别配置模拟主机加入 IPv6 组播组 FF1E::101。

```
[SwitchA] interface gigabitethernet 2/1/3
[SwitchA-GigabitEthernet2/1/3] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet2/1/3] quit
[SwitchA] interface gigabitethernet 2/1/4
[SwitchA-GigabitEthernet2/1/4] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet2/1/4] quit
```

4. 验证配置

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

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

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

VLAN 100: Total 1 entries.
  (::, FF1E::101)
    Host slots (0 in total):
    Host ports (2 in total):
      GE2/1/3        (00:03:23)
      GE2/1/4        (00:04:10)
```

由此可见，Host A 和 Host B 所在的端口 GigabitEthernet2/1/4 和 GigabitEthernet2/1/3 均已加入 IPv6 组播组 FF1E::101，但都未加入 IPv6 组播组 FF1E::202，这表明 IPv6 组播组过滤器已生效。

1.9.2 静态端口配置举例

1. 组网需求

- 如 图 1-4 所示，Router A通过GigabitEthernet2/1/2 接口连接IPv6 组播源（Source），通过GigabitEthernet2/1/1 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 GigabitEthernet2/1/3 和 GigabitEthernet2/1/5 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 GigabitEthernet2/1/3 配置为静

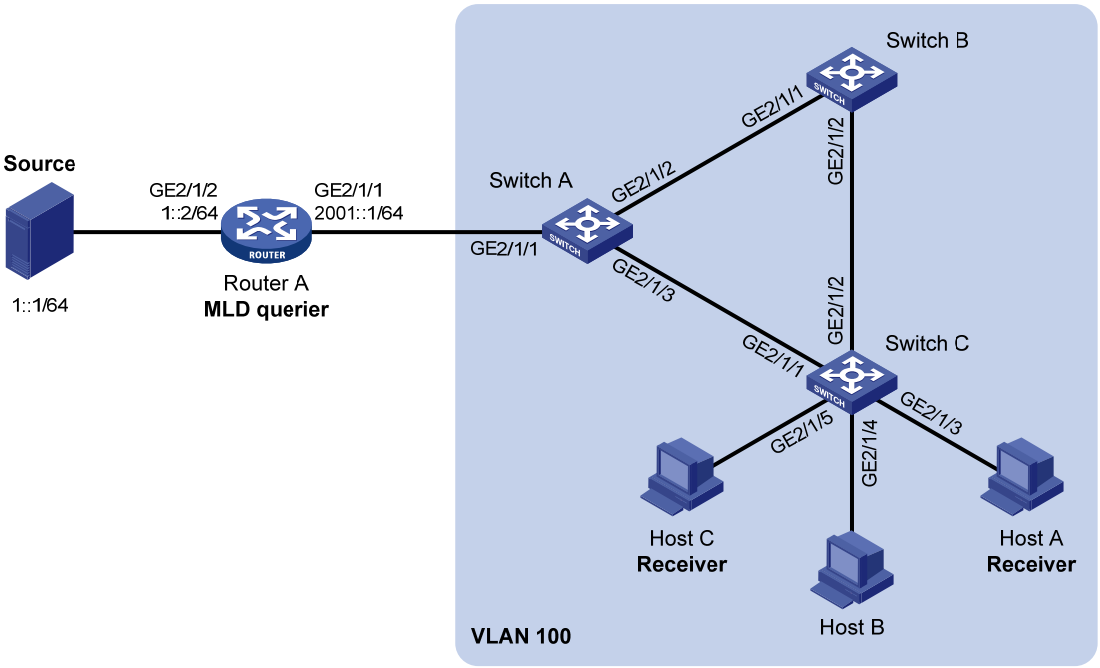
态路由器端口，以保证当 Switch A—Switch B—Switch C 的路径出现阻断时，IPv6 组播数据可以几乎不间断地通过 Switch A—Switch C 的新路径传递给接收者。

说明

- 如果没有配置静态路由器端口，那么当 Switch A—Switch B—Switch C 的路径出现阻断时，至少需要等待一个 MLD 查询和响应周期完成后，IPv6 组播数据才能通过 Switch A—Switch C 的新路径传递给接收者，IPv6 组播数据的传输在这个过程中将中断。
- 有关 STP（Spanning Tree Protocol，生成树协议）的详细介绍，请参见“二层技术-以太网交换配置指导”中的“生成树”。

2. 组网图

图1-4 静态端口配置组网图



3. 配置步骤

(1) 配置 IPv6 地址

请按照 图 1-4 配置各接口的IPv6 地址和前缀长度，具体配置过程略。

(2) 配置 Router A

使能 IPv6 组播路由，在接口 GigabitEthernet2/1/2 上使能 IPv6 PIM-DM，并在接口 GigabitEthernet2/1/1 上使能 MLD。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mld enable
[RouterA-GigabitEthernet2/1/1] quit
```

```
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ipv6 pim dm
[RouterA-GigabitEthernet2/1/2] quit
```

(3) 配置 Switch A

全局使能 MLD Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 到 GigabitEthernet2/1/3 添加到该 VLAN 中，并在该 VLAN 内使能 MLD Snooping。

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

把 GigabitEthernet2/1/3 配置为静态路由器端口。

```
[SwitchA] interface gigabitethernet 2/1/3
[SwitchA-GigabitEthernet2/1/3] mld-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet2/1/3] quit
```

(4) 配置 Switch B

全局使能 MLD Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 添加到该 VLAN 中，并在该 VLAN 内使能 MLD Snooping。

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

(5) 配置 Switch C

全局使能 MLD Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 到 GigabitEthernet2/1/5 添加到该 VLAN 中，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 2/1/1 to gigabitethernet 2/1/5
[SwitchC-vlan100] mld-snooping enable
[SwitchC-vlan100] quit
```

分别在端口 GigabitEthernet2/1/3 和 GigabitEthernet2/1/5 上配置静态加入 IPv6 组播组 FF1E::101。

```
[SwitchC] interface gigabitethernet 2/1/3
[SwitchC-GigabitEthernet2/1/3] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet2/1/3] quit
[SwitchC] interface gigabitethernet 2/1/5
```

```
[SwitchC-GigabitEthernet2/1/5] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet2/1/5] quit
```

4. 验证配置

显示 Switch A 上 VLAN 100 内静态路由器端口的信息。

```
[SwitchA] display mld-snooping static-router-port vlan 100
VLAN 100:
  Router slots (0 in total):
  Router ports (1 in total):
    GE2/1/3
```

由此可见，Switch A 上的端口 GigabitEthernet2/1/3 已经成为了静态路由器端口。

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

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

VLAN 100: Total 1 entries.
  (::, FF1E::101)
    Host slots (0 in total):
    Host ports (2 in total):
      GE2/1/3
      GE2/1/5
```

由此可见，Switch C 上的端口 GigabitEthernet2/1/3 和 GigabitEthernet2/1/5 已经成为了 IPv6 组播组 FF1E::101 的静态成员端口。

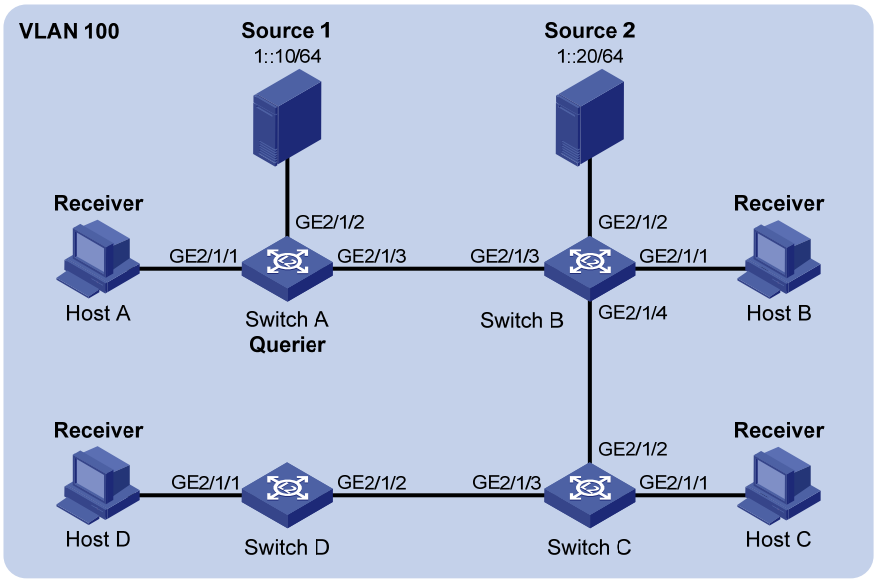
1.9.3 MLD Snooping查询器配置举例

1. 组网需求

- 如 图 1-5 所示，在一个没有三层设备的纯二层网络环境中，IPv6 组播源Source 1 和Source 2 分别向IPv6 组播组FF1E::101 和FF1E::102 发送IPv6 组播数据，Host A和Host C是IPv6 组播组FF1E::101 的接收者（Receiver），Host B和Host D则是IPv6 组播组FF1E::102 的接收者；所有接收者均使用MLDv1，所有交换机上都运行版本 1 的MLD Snooping，并选择距IPv6 组播源较近的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，在所有交换机上都使能丢弃未知 IPv6 组播数据报文功能。

2. 组网图

图1-5 MLD Snooping 查询器配置组网图



3. 配置步骤

(1) 配置 Switch A

全局使能 MLD Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 到 GigabitEthernet2/1/3 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并使能丢弃未知 IPv6 组播数据报文功能。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 2/1/1 to gigabitethernet 2/1/3
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping drop-unknown
```

在 VLAN 100 内使能 MLD Snooping 查询器。

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

(2) 配置 Switch B

全局使能 MLD Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 到 GigabitEthernet2/1/4 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并使能丢弃未知 IPv6 组播数据报文功能。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 2/1/1 to gigabitethernet 2/1/4
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] mld-snooping drop-unknown
```

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

(3) 配置 Switch C

全局使能 MLD Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 到 GigabitEthernet2/1/3 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并使能丢弃未知 IPv6 组播数据报文功能。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 2/1/1 to gigabitethernet 2/1/3
[SwitchC-vlan100] mld-snooping enable
[SwitchC-vlan100] mld-snooping drop-unknown
[SwitchC-vlan100] quit
```

(4) 配置 Switch D

全局使能 MLD Snooping。

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

创建 VLAN 100，把端口 GigabitEthernet2/1/1 到 GigabitEthernet2/1/2 添加到该 VLAN 中；在该 VLAN 内使能 MLD Snooping，并使能丢弃未知 IPv6 组播数据报文功能。

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

4. 验证配置

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

显示 Switch B 上收到的 MLD 报文的统计信息。

```
[SwitchB] display mld-snooping statistics
Received MLD general queries:  3
Received MLDv1 specific queries:  0
Received MLDv1 reports:  12
Received MLD dones:  0
Sent     MLDv1 specific queries:  0
Received MLDv2 reports:  0
Received MLDv2 reports with right and wrong records:  0
Received MLDv2 specific queries:  0
Received MLDv2 specific sg queries:  0
Sent     MLDv2 specific queries:  0
Sent     MLDv2 specific sg queries:  0
Received error MLD messages:  0
```

1.10 常见配置错误举例

1.10.1 二层设备不能实现二层组播

1. 故障现象

二层设备不能实现 MLD snooping 二层组播功能。

2. 故障分析

MLD Snooping 没有使能。

3. 处理过程

(1) 使用 **display mld-snooping** 命令查看 MLD Snooping 的运行状态。

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

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

1.10.2 配置的IPv6 组播组策略不生效

1. 故障现象

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

2. 故障分析

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

3. 处理过程

(1) 使用 **display acl ipv6** 命令查看所配置的 IPv6 ACL 规则，检查其是否与所要实现的 IPv6 组播组过滤策略相符合。

(2) 在 MLD-Snooping 视图或相应的接口视图下使用 **display this** 命令查看是否应用了正确的 IPv6 组播组策略。如果没有，则使用 **group-policy** 或 **mld-snooping group-policy** 命令应用正确的 IPv6 组播组策略。

(3) 使用 **display mld-snooping** 命令查看是否已使能丢弃未知 IPv6 组播数据报文的功能。如果没有使能，则使用 **drop-unknown** 或 **mld-snooping drop-unknown** 命令使能丢弃未知 IPv6 组播数据报文功能。

目 录

1 IPv6 组播路由与转发

1.1 IPv6组播路由与转发简介

IPv6 组播路由与转发中有以下三种表：

- 每个 IPv6 组播路由协议都有一个协议自身的路由表，如 IPv6 PIM 路由表。
- 各 IPv6 组播路由协议的 IPv6 组播路由信息经过综合形成一个总的 IPv6 组播路由表，该表由一系列（S，G）表项组成，即一系列由 IPv6 组播源 S 向 IPv6 组播组 G 发送 IPv6 组播数据的 IPv6 组播路由信息。IPv6 组播路由表中包含了由一或多种 IPv6 组播路由协议生成的 IPv6 组播路由。
- IPv6 组播转发表直接用于控制 IPv6 组播数据包的转发，它与 IPv6 组播路由表保持一致，IPv6 组播路由表中最优的 IPv6 组播路由会直接下发到 IPv6 组播转发表中。

1.1.1 RPF检查机制

IPv6 组播路由协议依赖于现有的 IPv6 单播路由信息或 IPv6 MBGP 路由来创建 IPv6 组播路由表项。IPv6 组播路由协议在创建 IPv6 组播路由表项时，运用了 RPF（Reverse Path Forwarding，逆向路径转发）检查机制，以确保 IPv6 组播数据能够沿正确的路径传输，同时还能避免由于各种原因而造成的环路。

1. RPF检查过程

执行 RPF 检查的依据是 IPv6 单播路由或 IPv6 MBGP 路由：

- IPv6 单播路由表中汇集了到达各个目的网段的最短路径；
- IPv6 MBGP 路由表直接提供 IPv6 组播路由信息。

在执行 RPF 检查时，路由器同时查找 IPv6 单播路由表和 IPv6 MBGP 路由表，具体过程如下：

(1) 首先，分别从 IPv6 单播路由表和 IPv6 MBGP 路由表中各选出一条最优路由：

- 以“报文源”的 IPv6 地址为目的地址查找 IPv6 单播路由表，自动选取一条最优 IPv6 单播路由。对应表项中的出接口为 RPF 接口，下一跳为 RPF 邻居。路由器认为来自 RPF 邻居且由该 RPF 接口收到的 IPv6 组播报文所经历的路径是从源 S 到本地的最短路径。
- 以“报文源”的 IPv6 地址为目的地址查找 IPv6 MBGP 路由表，自动选取一条最优 IPv6 MBGP 路由。对应表项中的出接口为 RPF 接口，下一跳为 RPF 邻居。

(2) 然后，从这两条最优路由中选择一条作为 RPF 路由：

- 如果配置了按照最长匹配选择路由，则从这两条路由中选出最长匹配的那条路由；如果这两条路由的前缀长度一样，则选择其中路由优先级最高的那条路由；如果它们的路由优先级也相同，则按照 IPv6 MBGP 路由、IPv6 单播路由的顺序进行选择。有关路由优先级的详细介绍，请参见“三层技术-IP 路由配置指导”中的“IP 路由基础”。
- 如果没有配置按照最长匹配选择路由，则从这两条路由中选出路由优先级最高的那条路由；如果它们的路由优先级相同，则按照 IPv6 MBGP 路由、IPv6 单播路由的顺序进行选择。

说明

根据 IPv6 组播报文传输的具体情况不同，“报文源”所代表的具体含义也不同：

- 如果当前报文沿从组播源到接收者或 RP（Rendezvous Point，汇集点）的 SPT（Shortest Path Tree，最短路径树）进行传输，则以组播源为“报文源”进行 RPF 检查；
- 如果当前报文沿从 RP 到接收者的 RPT（Rendezvous Point Tree，共享树）进行传输，或者沿从组播源到 RP 的组播源侧 RPT 进行传输，则都以 RP 为“报文源”进行 RPF 检查；
- 如果当前报文为 BSR（Bootstrap Router，自举路由器）报文，沿从 BSR 到各路由器的路径进行传输，则以 BSR 为“报文源”进行 RPF 检查。

有关 SPT、RPT、组播源侧 RPT、RP 和 BSR 的详细介绍，请参见“IP 组播配置指导”中的“IPv6 PIM”。

2. RPF检查在IPv6 组播转发中的应用

对每一个收到的 IPv6 组播数据报文都进行 RPF 检查会给路由器带来较大负担，而利用 IPv6 组播转发表可以解决这个问题。在建立 IPv6 组播路由和转发表时，会把 IPv6 组播数据报文（S，G）的 RPF 接口记录为（S，G）表项的入接口。当路由器收到 IPv6 组播数据报文（S，G）后，查找 IPv6 组播转发表：

(1) 如果 IPv6 组播转发表中不存在（S，G）表项，则对该报文执行 RPF 检查，将其 RPF 接口作为入接口，结合相关路由信息创建相应的表项，并下发到 IPv6 组播转发表中：

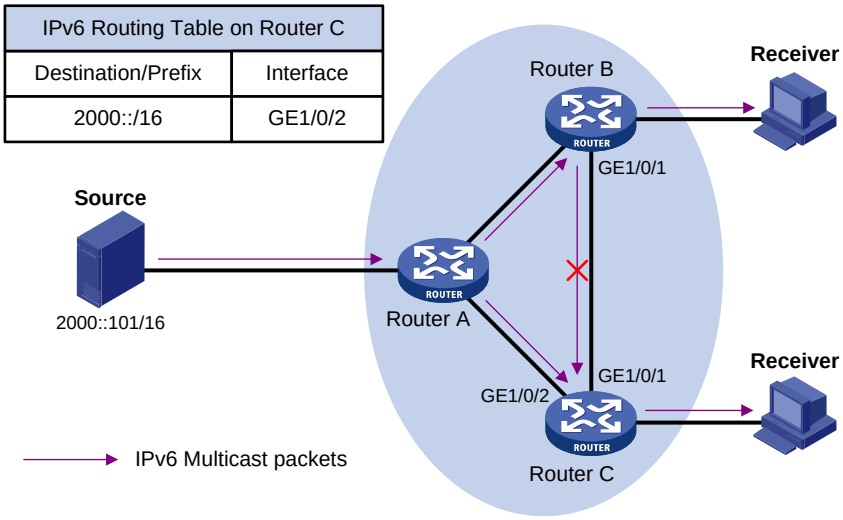
- 若该报文实际到达的接口正是其 RPF 接口，则 RPF 检查通过，向所有的出接口转发该报文；
- 若该报文实际到达的接口不是其 RPF 接口，则 RPF 检查失败，丢弃该报文。

(2) 如果 IPv6 组播转发表中已存在（S，G）表项，且该报文实际到达的接口与入接口相匹配，则向所有的出接口转发该报文。

(3) 如果 IPv6 组播转发表中已存在（S，G）表项，但该报文实际到达的接口与入接口不匹配，则对此报文执行 RPF 检查：

- 若其 RPF 接口与入接口一致，则说明（S，G）表项正确，丢弃这个来自错误路径的报文；
- 若其 RPF 接口与入接口不符，则说明（S，G）表项已过时，于是把入接口更新为 RPF 接口。如果该报文实际到达的接口正是其 RPF 接口，则向所有的出接口转发该报文，否则将其丢弃。

图1-1 RPF 检查过程



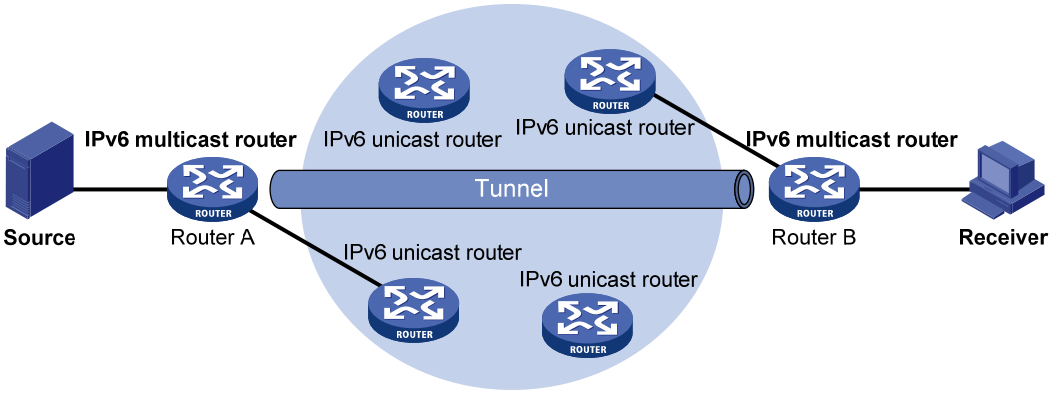
如 图 1-1 所示，假设网络中IPv6 单播路由畅通，未配置IPv6 MBGP。IPv6 组播报文（S，G）沿从组播源（Source）到接收者（Receiver）的SPT进行传输。假定Router C上的IPv6 组播转发表中已存在（S，G）表项，其记录的入接口为GigabitEthernet1/0/2：

- 如果该 IPv6 组播报文从接口 GigabitEthernet1/0/2 到达 Router C，与（S，G）表项的入接口相匹配，则向所有的出接口转发该报文。
- 如果该 IPv6 组播报文从接口 GigabitEthernet1/0/1 到达 Router C，与（S，G）表项的入接口不匹配，则对其执行 RPF 检查：通过查找 IPv6 单播路由表发现到达 Source 的出接口（即 RPF 接口）是 GigabitEthernet1/0/2，与（S，G）表项的入接口一致。这说明（S，G）表项是正确的，该报文来自错误的路径，RPF 检查失败，于是丢弃该报文。

1.1.2 跨IPv6 单播网段的IPv6 组播转发

网络中可能存在不支持 IPv6 组播协议的路由器，从 IPv6 组播源发出的 IPv6 组播数据沿 IPv6 组播路由器逐跳转发，当下一跳路由器不支持 IPv6 组播协议时，IPv6 组播转发路径将被阻断。而通过在处于 IPv6 单播网段两端的 IPv6 组播路由器之间建立隧道，则可以实现跨 IPv6 单播网段的 IPv6 组播数据转发。

图1-2 使用隧道传输 IPv6 组播数据



如 图 1-2 所示，在IPv6 组播路由器Router A和Router B之间建立隧道。Router A将IPv6 组播数据封装在IPv6 单播报文中，通过IPv6 单播路由器转发至隧道另一端的Router B，再由Router B将IPv6 单播报文头剥掉后继续进行IPv6 组播传输。

1.2 IPv6组播路由与转发配置任务简介

表1-1 IPv6 组播路由与转发配置任务简介

配置任务		说明	详细配置
使能IPv6组播路由		必选	1.3
配置IPv6组播路由与转发	配置按照最长匹配选择RPF路由	可选	1.4.2
	配置对IPv6组播流量进行负载分担	可选	1.4.3
	配置IPv6组播转发边界	可选	1.4.4

1.3 使能IPv6组播路由

在公网实例或 VPN 实例中配置各项三层 IPv6 组播功能之前，必须先在该实例中使能 IPv6 组播路由。

表1-2 使能 IPv6 组播路由

操作	命令	说明
进入系统视图	**system-view**	-
使能IPv6组播路由，并进入IPv6 MRIB（Multicast Routing Information Base，组播路由信息库）视图	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	缺省情况下，IPv6组播路由处于关闭状态

1.4 配置IPv6组播路由与转发

1.4.1 配置准备

在配置 IPv6 组播路由与转发之前，需完成以下任务：

- 配置任一 IPv6 单播路由协议，实现域内网络层互通
- 配置 IPv6 PIM-DM 或 IPv6 PIM-SM

1.4.2 配置按照最长匹配选择RPF路由

用户可以配置组播路由器按照最长匹配原则来选择RPF路由，有关RPF路由选择的详细介绍，请参见“1.1.1 1. RPF检查过程”一节。

表1-3 配置按照最长匹配选择 RPF 路由

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 MRIB视图	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	-
配置按照最长匹配选择RPF路由	**longest-match**	缺省情况下，选择路由优先级最高的路由作为RPF路由

1.4.3 配置对IPv6 组播流量进行负载分担

用户通过配置根据组播源或组播源组进行 IPv6 组播流量的负载分担，可以优化存在多条 IPv6 组播数据流时的网络流量。

表1-4 配置对 IPv6 组播流量进行负载分担

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 MRIB视图	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	-
配置对IPv6组播流量进行负载分担	**load-splitting** { **source** | **source-group** }	缺省情况下，不对IPv6组播流量进行负载分担

1.4.4 配置IPv6 组播转发边界

提示

进行本配置不需要使能 IPv6 组播路由。

IPv6 组播信息在网络中的转发并不是漫无边际的，每个 IPv6 组播组对应的 IPv6 组播信息都必须在确定的范围内传递。IPv6 组播转发边界为指定范围或 Scope 值的 IPv6 组播组划定了边界条件，如果 IPv6 组播报文的目的地址与边界条件匹配，就停止转发。当在一个接口上配置了 IPv6 组播转发边界后，将不能从该接口转发 IPv6 组播报文（包括本机发出的 IPv6 组播报文），也不能从该接口接收 IPv6 组播报文。

表1-5 配置 IPv6 组播转发边界

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置IPv6组播转发边界	**ipv6 multicast boundary** { *ipv6-group-address prefix-length* | **scope** { *scope-id* | **admin-local** | **global** | **organization-local** | **site-local** } }	缺省情况下，没有配置IPv6组播转发边界

1.5 IPv6组播路由与转发显示和维护

注意

执行 **reset** 命令清除 IPv6 组播路由表或 IPv6 组播转发表中的信息，可能导致 IPv6 组播信息无法正常传输。

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 组播路由与转发的运行情况，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 组播路由与转发的统计信息。

表1-6 IPv6 组播路由与转发显示和维护

操作	命令
显示IPv6 MRIB维护的接口信息	**display ipv6 mrib** [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*]
显示IPv6组播边界的信息	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **boundary** { **group** [*ipv6-group-address* [*prefix-length*]] | **scope** [*scope-id*] } [**interface** *interface-type interface-number*]
显示IPv6组播转发的DF信息（MSR 2600/MSR 3600）	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding df-info** [*ipv6-rp-address*] [**verbose**]
显示IPv6组播转发的DF信息（MSR 5600）	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding df-info** [*ipv6-rp-address*] [**verbose**] [**slot** *slot-number*]
显示IPv6组播转发的事件统计信息（MSR 2600/MSR 3600）	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding event**
显示IPv6组播转发的事件统计信息（MSR 5600）	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding event** [**slot** *slot-number*]

操作	命令
显示IPv6组播转发表的信息（MSR 2600/MSR 3600）	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number* | **statistics**] *
显示IPv6组播转发表的信息（MSR 5600）	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **cpu** *cpu-number* | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number* | **slot** *slot-number* | **statistics**] *
显示IPv6组播转发表的DF列表信息（MSR 2600/MSR 3600）	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table df-list** [*ipv6-group-address*] [**verbose**]
显示IPv6组播转发表的DF列表信息（MSR 5600）	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table df-list** [*ipv6-group-address*] [**verbose**] [**slot** *slot-number*]
显示IPv6组播路由表的信息	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **routing-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *
显示IPv6组播源的RPF信息	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **rpf-info** *ipv6-source-address* [*ipv6-group-address*]
清除IPv6组播转发的事件统计信息	**reset ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding event**
清除IPv6组播转发表中的转发项	**reset ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table** { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* } } * | **all** }
清除IPv6组播路由表中的路由项	**reset ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **routing-table** { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** *interface-type interface-number* } * | **all** }

说明

- 清除 IPv6 组播路由表中的路由项后，IPv6 组播转发表中的相应表项也将随之删除。
- 清除 IPv6 组播转发表中的转发项后，IPv6 组播路由表中的相应表项也将随之删除。

1.6 IPv6组播路由与转发典型配置举例

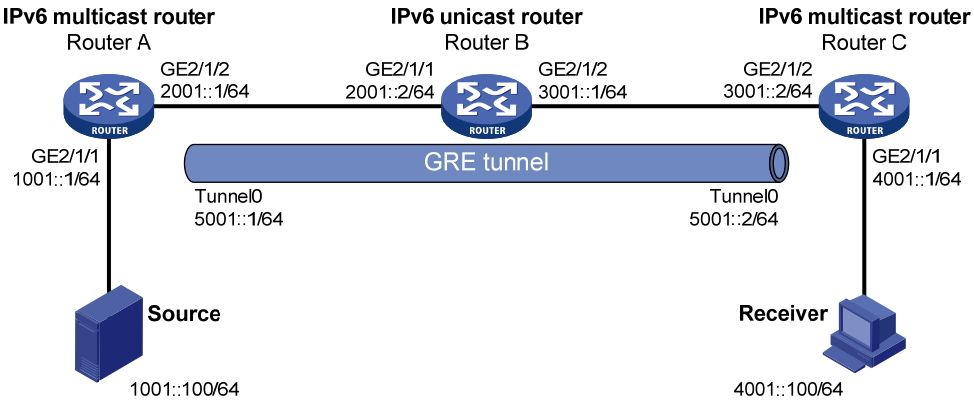
1.6.1 利用GRE隧道实现IPv6 组播转发配置举例

1. 组网需求

- Router A 和 Router C 支持 IPv6 组播功能并运行 IPv6 PIM-DM，但 Router B 不支持 IPv6 组播功能；
- Router A、Router B 和 Router C 之间运行 OSPFv3 协议；
- 要求通过配置，使 Receiver 能够接收来自 Source 的 IPv6 组播信息。

2. 组网图

图1-3 利用 GRE 隧道实现 IPv6 组播转发配置组网图



3. 配置步骤

(1) 配置 IPv6 地址和 IPv6 单播路由协议

请按照 图 1-3 配置各接口的IPv6 地址和前缀长度，具体配置过程略。

配置各路由器之间采用 OSPFv3 协议进行互连，确保各路由器之间在网络层互通，并能够借助 IPv6 单播路由协议实现动态路由更新，具体配置过程略。

(2) 配置 GRE 隧道

在 Router A 上创建接口 Tunnel0，并指定其隧道模式为 GRE over IPv6 隧道。

```
<RouterA> system-view
[RouterA] interface tunnel 0 mode gre ipv6
```

在 Router A 上为 Tunnel0 接口配置 IPv6 地址，并指定隧道的源地址和目的地址。

```
[RouterA-Tunnel0] ipv6 address 5001::1 64
[RouterA-Tunnel0] source 2001::1
[RouterA-Tunnel0] destination 3001::2
[RouterA-Tunnel0] quit
```

在 Router C 上创建接口 Tunnel0，并指定其隧道模式为 GRE over IPv6 隧道。

```
<RouterC> system-view
[RouterC] interface tunnel 0 mode gre ipv6
```

在 Router C 上为 Tunnel0 接口配置 IPv6 地址，并指定隧道的源地址和目的地址。

```
[RouterC-Tunnel0] ipv6 address 5001::2 64
[RouterC-Tunnel0] source 3001::2
[RouterC-Tunnel0] destination 2001::1
[RouterC-Tunnel0] quit
```

(3) 使能 IPv6 组播路由，并使能 IPv6 PIM-DM 和 MLD

在 Router A 上使能 IPv6 组播路由，并在各接口上使能 IPv6 PIM-DM。

```
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ipv6 pim dm
[RouterA-GigabitEthernet2/1/1] quit
```

```
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ipv6 pim dm
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] interface tunnel 0
[RouterA-Tunnel0] ipv6 pim dm
[RouterA-Tunnel0] quit
```

在 Router C 上使能 IPv6 组播路由，在主机侧接口 GigabitEthernet2/1/1 上使能 MLD，并在其它接口上使能 IPv6 PIM-DM。

```
[RouterC] ipv6 multicast routing
[RouterC-mrib6] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mld enable
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface gigabitethernet 2/1/2
[RouterC-GigabitEthernet2/1/2] ipv6 pim dm
[RouterC-GigabitEthernet2/1/2] quit
[RouterC] interface tunnel 0
[RouterC-Tunnel0] ipv6 pim dm
[RouterC-Tunnel0] quit
```

4. 验证配置

IPv6 组播源向 IPv6 组播组 FF1E::101 发送 IPv6 组播数据，接收者加入该 IPv6 组播组后能够收到 IPv6 组播源发来的 IPv6 组播数据。通过使用 **display ipv6 pim routing-table** 命令可以查看路由器的 IPv6 PIM 路由表信息。例如：

显示 Router C 上的 IPv6 PIM 路由表信息。

```
[RouterC] display ipv6 pim routing-table
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, FF1E::101)
     Protocol: pim-dm, Flag: WC
     UpTime: 00:04:25
     Upstream interface: NULL
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/1/1
             Protocol: mld, UpTime: 00:04:25, Expires: -

 (1001::100, FF1E::101)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:06:14
     Upstream interface: Tunnel0
         Upstream neighbor: FE80::A01:101:1
         RPF prime neighbor: FE80::A01:101:1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/1/1
```

```
        Protocol: pim-dm, UpTime: 00:04:25, Expires: -
```

Router C 的 RPF 邻居为 Router A，IPv6 组播数据通过 GRE 隧道由直接 Router A 发往 Router C。

目 录

1 MLD

说明

SIC-4FSW/4FSWP 和 SIC-9FSW/9FSWP 交换卡不支持 MLD。

1.1 MLD简介

MLD（Multicast Listener Discovery Protocol，组播侦听者发现协议）用于在三层设备和其直连网段中的用户主机之间建立和维护 IPv6 组播组成员关系。

1.1.1 MLD的版本

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 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，而 MLDv1 则需要在 MLD SSM Mapping 技术的支持下才能应用于 SSM 模型。有关 ASM 和 SSM 模型的介绍，请参见“IP 组播配置指导”中的“组播概述”。

1.1.2 MLDv1 工作机制

MLDv1 主要基于查询和响应机制完成对 IPv6 组播组成员的管理。

1. 查询器选举机制

当一个网段内有多台运行 MLD 的路由器时，由于它们都能从主机那里收到 MLD 成员关系报告报文（Multicast Listener Report Message），因此只需其中一台路由器发送 MLD 查询报文（Query Message）即可，该路由器就称为 MLD 查询器（Querier）。这就需要有一个查询器的选举机制来确定由哪台路由器作为 MLD 查询器，其选举过程如下：

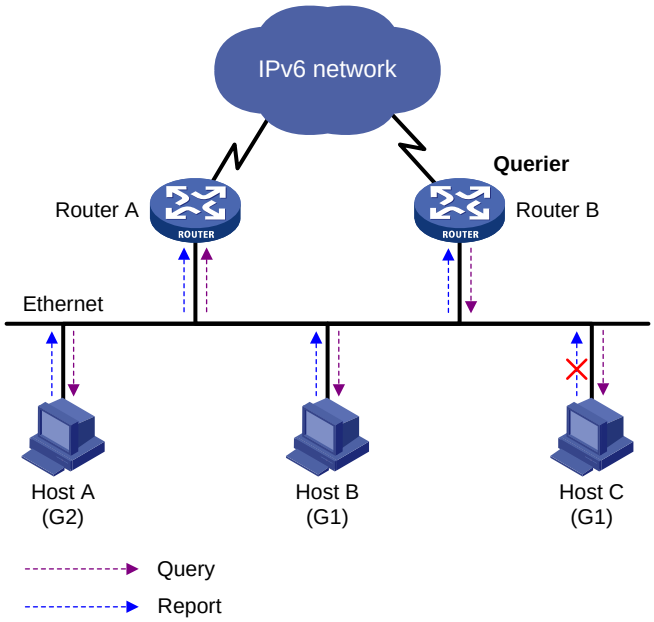
(1) 所有 MLD 路由器在初始时都认为自己是查询器，并向本地网段内的所有主机和路由器发送 MLD 普遍组查询（General Query）报文（目的地址为 FF02::1）；

(2) 本地网段中的其它 MLD 路由器在收到该报文后，将报文的源 IPv6 地址与自己的链路本地接口地址作比较。通过比较，IPv6 地址最小的路由器将成为查询器，其它路由器成为非查询器（Non-Querier）；

(3) 所有非查询器上都会启动一个定时器（即其它查询器存在时间定时器 Other Querier Present Timer）。在定时器超时前，如果收到了来自查询器的 MLD 查询报文，则重置该定时器；否则，就认为原查询器失效，并发起新的查询器选举过程。

2. 加入IPv6 组播组机制

图1-1 MLD 查询响应示意图



如 图 1-1 所示，假设Host B与Host C想要收到发往IPv6 组播组G1 的IPv6 组播数据，而Host A想要收到发往IPv6 组播组G2 的IPv6 组播数据，那么主机加入IPv6 组播组以及MLD查询器（Router B）维护IPv6 组播组成员关系的基本过程如下：

(1) 主机会主动向其要加入的 IPv6 组播组发送 MLD 成员关系报告报文以声明加入，而不必等待 MLD 查询器发来的 MLD 查询报文；

(2) MLD 查询器（Router B）周期性地以组播方式向本地网段内的所有主机和路由器发送普遍组查询报文（目的地址为 FF02::1）；

(3) 在收到该查询报文后，关注 G1 的 Host B 与 Host C 其中之一（这取决于谁的延迟定时器先超时）——譬如 Host B 会首先以组播方式向 G1 发送 MLD 成员关系报告报文，以宣告其属于 G1。由于本地网段中的所有主机都能收到 Host B 发往 G1 的报告报文，因此当 Host C 收到该报告报文后，将不再发送同样针对 G1 的报告报文，因为 MLD 路由器（Router A 和 Router B）已知道本地网段中有对 G1 感兴趣的主机了。这个机制称为主机上的 MLD 成员关系报告抑制机制，该机制有助于减少本地网段的信息流量；

(4) 与此同时，由于 Host A 关注的是 G2，所以它仍将以组播方式向 G2 发送报告报文，以宣告其属于 G2；

(5) 经过以上的查询和响应过程，MLD 路由器了解到本地网段中有 G1 和 G2 的成员，于是由 IPv6 组播路由协议（如 IPv6 PIM）生成（*，G1）和（*，G2）组播转发项作为 IPv6 组播数据的转发依据，其中的“*”代表任意 IPv6 组播源；

(6) 当由 IPv6 组播源发往 G1 或 G2 的 IPv6 组播数据经过组播路由到达 MLD 路由器时，由于 MLD 路由器上存在（*，G1）和（*，G2）组播转发项，于是将该 IPv6 组播数据转发到本地网段，接收者主机便能收到该 IPv6 组播数据了。

3. 离开IPv6 组播组机制

当一个主机离开某 IPv6 组播组时：

(1) 该主机向本地网段内的所有 IPv6 组播路由器（目的地址为 FF02::2）发送离开组（Done）报文；

(2) 当查询器收到该报文后，向该主机所声明要离开的那个 IPv6 组播组发送特定组查询（Multicast-Address-Specific Query）报文（目的地址字段和组地址字段均填充为所要查询的 IPv6 组播组地址）；

(3) 如果该网段内还有该 IPv6 组播组的其它成员，则这些成员在收到特定组查询报文后，会在该报文中所设定的最大响应时间（Maximum Response Delay）内发送成员关系报告报文；

(4) 如果在最大响应时间内收到了该 IPv6 组播组其它成员发送的成员关系报告报文，查询器就会继续维护该 IPv6 组播组的成员关系；否则，查询器将认为该网段内已无该 IPv6 组播组的成员，于是不再维护这个 IPv6 组播组的成员关系。

1.1.3 MLDv2 的改进

MLDv2 在兼容和继承 MLDv1 的基础上，进一步增强了主机的控制能力，并增强了 MLD 状态。

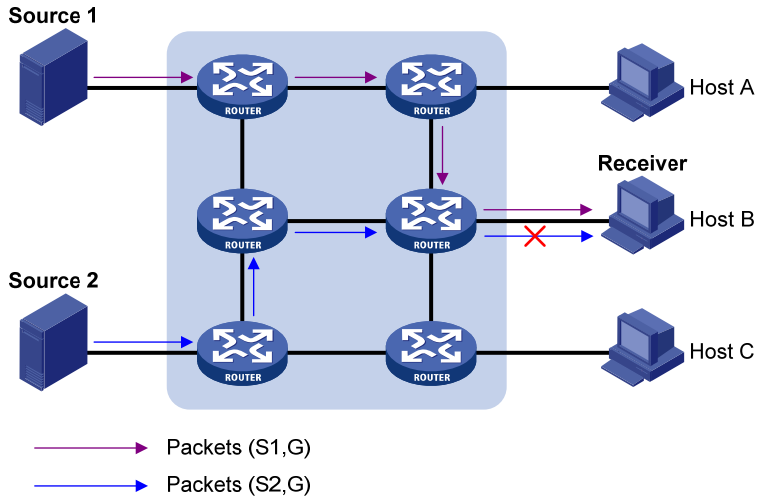
1. 主机控制能力的增强

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，则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，……）。

如 图 1-2 所示，网络中存在Source 1（S1）和Source 2（S2）两个IPv6 组播源，均向IPv6 组播组G发送IPv6 组播报文。Host B仅对从Source 1 发往G的信息感兴趣，而对来自Source 2 的信息没有兴趣。

图1-2 指定源组的 IPv6 组播流路经



如果主机与路由器之间运行的是 MLDv1，Host B 加入 IPv6 组播组 G 时无法对 IPv6 组播源进行选择，因此无论 Host B 是否需要，来自 Source 1 和 Source 2 的 IPv6 组播信息都将传递给 Host B。

当主机与路由器之间运行了 MLDv2 之后，Host B 就可以要求只接收来自 Source 1、发往 G 的 IPv6 组播信息（S1，G），或要求拒绝来自 Source 2、发往 G 的 IPv6 组播信息（S2，G），这样就只有来自 Source 1 的 IPv6 组播信息才能传递给 Host B 了。

2. MLD状态的增强

运行 MLDv2 的组播路由器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：

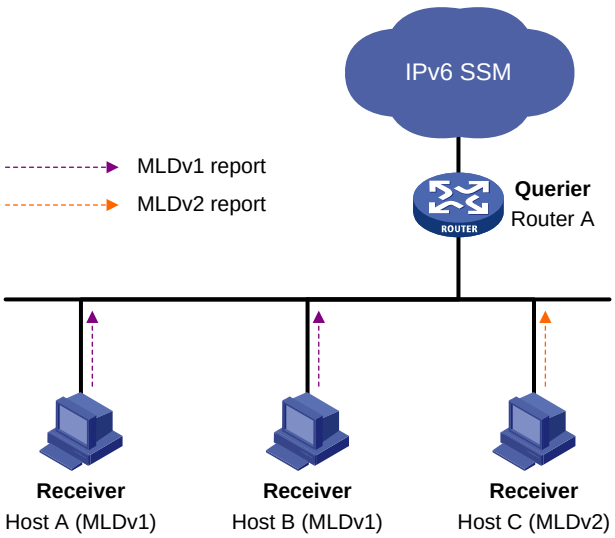
- 过滤模式：保持对 INCLUDE 或 EXCLUDE 的状态跟踪。
- 源列表：保持对新增或删除 IPv6 组播源的跟踪。
- 定时器：表示 IPv6 组播地址超时后切换到 INCLUDE 模式的过滤定时器、关于源记录的源定时器等。

1.1.4 MLD SSM Mapping

MLD SSM Mapping 通过在路由器上配置 SSM 静态映射规则，从而为运行 MLDv1 的接收者主机提供对 SSM 模型的支持。

SSM 模型要求在接收者主机所在的网段，路由器能够了解主机加入 IPv6 组播组时所指定的 IPv6 组播源。如果接收者主机上运行的是 MLDv2，则可以在 MLDv2 的报告报文中直接指定 IPv6 组播源的地址；如果某些接收者主机只能运行 MLDv1，则在 MLDv1 的报告报文中无法指定 IPv6 组播源的地址。这种情况下需要通过在路由器上配置 MLD SSM Mapping 规则，将 MLDv1 报告报文中所包含的（*，G）信息映射为（G，INCLUDE，（S1，S2...））信息。

图1-3 MLD SSM Mapping 组网图



在如 图 1-3 所示的IPv6 SSM网络中，Host A、Host B和Host C上分别运行MLDv1 和MLDv2。在不允许将Host A和Host B升级为MLDv2 的情况下，若要为Host A和Host B也提供SSM组播服务，则需在Router A上配置MLD SSM Mapping规则。

配置完成后，当 Router A 收到来自主机的 MLDv1 报告报文时，首先检查该报文中所携带的 IPv6 组播组地址 G，然后根据检查结果的不同分别进行处理：

(1) 如果 G 不在 IPv6 SSM 组地址范围内，则提供 ASM 组播服务。

(2) 如果 G 在 IPv6 SSM 组地址范围内：

- 若 Router A 上没有 G 对应的 MLD SSM Mapping 规则，则无法提供 SSM 组播服务，丢弃该报文；
- 若 Router A 上有 G 对应的 MLD SSM Mapping 规则，则依据规则将报告报文中所包含的(*，G）信息映射为（G，INCLUDE，（S1，S2...））信息，可以提供 SSM 组播服务。

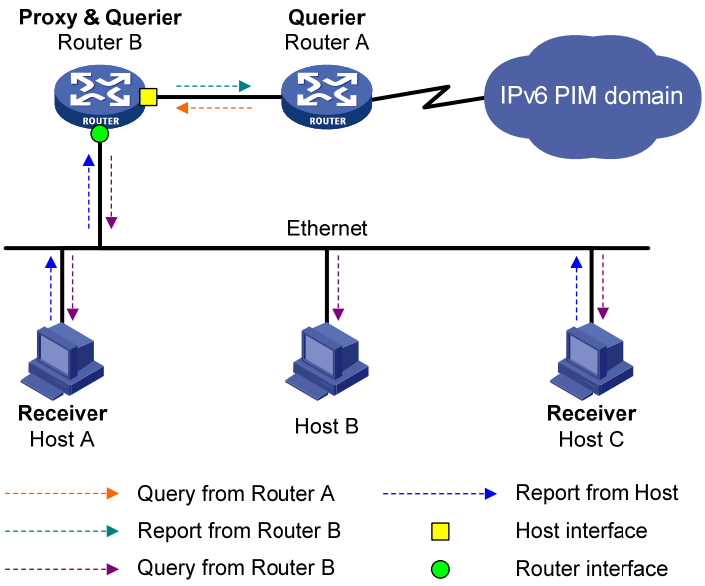
说明

- MLD SSM Mapping 不对 MLDv2 的报告报文进行处理。
- 有关 IPv6 SSM 组地址范围的介绍，请参见“IP 组播配置指导”中的“IPv6 PIM”。

1.1.5 MLD代理

在一些简单的树型网络拓扑中，边缘设备上并不需要运行复杂的 IPv6 组播路由协议（如 IPv6 PIM），可以通过在这些设备上配置 MLD 代理，使其代理下游主机来发送 MLD 报文及维护组成员关系，并基于该关系进行组播转发。在上游设备看来，配置了 MLD 代理功能的设备（称为 MLD 代理设备）不再是一个 IPv6 PIM 邻居，而只是一台主机。

图1-4 MLD 代理组网图



如 图 1-4 所示，MLD代理中定义了以下两种接口类型：

- 上行接口：又称代理接口，指 MLD 代理设备上运行 MLD 代理功能的接口，即朝向组播分发树树根方向的接口。由于该接口执行 MLD 协议的主机行为，因此也称为主机接口（Host Interface）。
- 下行接口：指 MLD 代理设备上除上行接口外其它运行 MLD 协议的接口，即背向组播分发树树根方向的接口。由于该接口执行 MLD 协议的路由器行为，因此也称为路由器接口（Router Interface）。

MLD 代理设备上维护着一个组成员关系数据库（Membership Database），将所有下行接口维护的组成员关系记录都存到这个数据库中。组成员关系记录的结构如下：（Multicast-address，Filter-mode，Source-list），每条记录都是各下行接口上具有相同组地址的成员关系记录的合集。

上行接口正是依据这个数据库来执行主机行为——当收到查询报文时根据当前数据库状态响应报告报文，或者当数据库变化时主动发送报告或离开报文；而下行接口则执行路由器行为——参与查询器的选举、发送查询报文并根据报告报文维护组成员关系等。

1.1.6 多实例的MLD

MLD 依据接口来维护组成员关系，各实例的 MLD 根据接口所属的实例来处理协议报文的收发。当路由器收到 MLD 报文时，需要区分该报文所属的实例，并在该实例范围内对其进行处理。当某实例内的 MLD 需要和其它 IPv6 组播协议交互信息时，只会通知本实例内的其它 IPv6 组播协议。

1.1.7 协议规范

与 MLD 相关的协议规范有：

- RFC 2710：Multicast Listener Discovery (MLD) for IPv6
- RFC 3810：Multicast Listener Discovery Version 2 (MLDv2) for IPv6

1.2 MLD配置任务简介

表1-1 MLD 配置任务简介

配置任务		说明	详细配置
配置MLD基本功能	使能MLD	必选	1.3.2
	配置MLD版本	可选	1.3.3
	配置静态加入	可选	1.3.4
	配置IPv6组播组过滤器	可选	1.3.5
调整MLD性能	配置MLD查询	可选	1.4.2
	配置IPv6组播组成员快速离开	可选	1.4.3
配置MLD SSM Mapping		可选	1.5.2
配置MLD代理	使能MLD代理功能	可选	1.6.2
	配置非查询器转发功能	可选	1.6.3
	配置MLD代理的负载分担功能	可选	1.6.4

1.3 配置MLD基本功能

1.3.1 配置准备

在配置 MLD 基本功能之前，需完成以下任务：

- 配置任一 IPv6 单播路由协议，实现网络层互通

- 配置 IPv6 PIM 协议

在配置 MLD 基本功能之前，需准备以下数据：

- MLD 的版本
- 以静态方式加入的 IPv6 组播组和 IPv6 组播源的地址
- IPv6 组播组过滤的 ACL 规则

1.3.2 使能MLD

在需要建立和维护 IPv6 组播组成员关系的接口上使能 MLD。

表1-2 使能 MLD

操作	命令	说明
进入系统视图	**system-view**	-
使能IPv6组播路由，并进入IPv6 MRIB视图	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	缺省情况下，IPv6组播路由处于关闭状态 本命令的详细介绍请参见“IP组播命令参考”中的“IPv6组播路由与转发”
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能MLD	**mld enable**	缺省情况下，没有使能MLD

1.3.3 配置MLD版本

由于不同版本 MLD 协议的报文结构与种类不同，因此需要为同一网段上的所有路由器配置相同版本的 MLD，否则 MLD 将不能正常运行。

表1-3 配置 MLD 版本

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置MLD的版本	**mld version** *version-number*	缺省情况下，MLD的版本为MLDv1

1.3.4 配置静态加入

在配置了静态加入 IPv6 组播组或组播源组后，接口将作为该 IPv6 组播组的虚拟组成员存在，从而可以接收发往该组的 IPv6 组播数据，以测试 IPv6 组播数据的转发。

在配置了静态加入后，接口并不会对 MLD 查询器发出的查询报文进行响应；当配置静态加入或取消静态加入的配置时，接口也不会主动发送 MLD 成员关系报告报文或 MLD 离开组报文。也就是说，该接口并没有真正成为该 IPv6 组播组的成员。

提示

在运行IPv6 PIM-SM的设备上配置静态加入时，如果待配接口上同时使能了MLD和IPv6 PIM-SM，则该接口必须为 IPv6 PIM-SM 的 DR，否则该接口将不能加入 IPv6 组播组或组播源组；如果待配接口上使能了 MLD 但未使能 IPv6 PIM-SM，则该接口必须为 MLD 查询器，否则该接口也不能加入 IPv6 组播组或组播源组。有关 IPv6 PIM-SM 和 DR 的介绍，请参见“IP 组播配置指导”中的“IPv6 PIM”。

表1-4 配置静态加入

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置静态加入IPv6组播组或组播源组	**mld static-group** *ipv6-group-address* [**source** *ipv6-source-address*]	缺省情况下，接口没有以静态方式加入任何IPv6组播组或组播源组

1.3.5 配置IPv6 组播组过滤器

如果不希望接口所在网段上的主机加入某些 IPv6 组播组，可在该接口上配置 IPv6 ACL 规则作为过滤器，接口将按照该规则对收到的 MLD 成员关系报告报文进行过滤，只为该规则所允许的 IPv6 组播组维护组成员关系。

表1-5 配置 IPv6 组播组过滤器

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置IPv6组播组过滤器	**mld group-policy** *acl6-number* [*version-number*]	缺省情况下，接口上没有配置IPv6组播组过滤器，即该接口下的主机可以加入任意IPv6组播组

说明

由于 IPv6 组播组过滤器只能过滤 MLD 报文，因此无法对接口静态加入 IPv6 组播组或组播源组进行限制。

1.4 调整MLD性能

1.4.1 配置准备

在调整 MLD 性能之前，需完成以下任务：

- 配置任一 IPv6 单播路由协议，实现网络层互通
- 配置 MLD 基本功能

1.4.2 配置MLD查询

MLDv1/v2 查询器会周期性地发送 MLD 普遍组查询报文，以判断网络上是否有 IPv6 组播组成员，发送间隔即为“MLD 普遍组查询报文的发送间隔”，可以根据网络的实际情况来修改此间隔。

当同一网段上有多台 IPv6 组播路由器时，由 MLD 查询器负责发送 MLD 查询报文。如果非查询器在“其它查询器存在时间”超时前未收到来自查询器的 MLD 查询报文，就会认为原查询器失效，从而触发新的查询器选举过程；否则，非查询器将重置“其它查询器存在时间定时器”。

提示

应确保 MLD 其它查询器的存在时间大于 MLD 普遍组查询报文的发送间隔，否则有可能导致网络内的 MLD 查询器反复变化。

表1-6 配置 MLD 查询

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置MLD普遍组查询报文的发送间隔	**mld query-interval** *interval*	缺省情况下，MLD普遍组查询报文的发送间隔为125秒
配置MLD其它查询器的存在时间	**mld other-querier-present-interval** *interval*	缺省情况下，MLD其它查询器的存在时间＝MLD普遍组查询报文的发送间隔×MLD查询器的健壮系数＋MLD普遍组查询的最大响应时间÷2

1.4.3 配置IPv6 组播组成员快速离开

在某些应用（如 ADSL 拨号上网）中，MLD 查询器的一个端口唯一对应着一台接收者主机，当主机在多个 IPv6 组播组间频繁切换（如进行电视选台）时，为了快速响应主机的离开组报文，可以在 MLD 查询器上开启 MLD 快速离开功能。

在使能了 MLD 快速离开功能之后，当 MLD 查询器收到来自主机的离开组报文时，不再发送 MLD 特定组查询报文或 MLD 特定源组查询报文，而是直接向上游发送离开通告，这样一方面减小了响应延迟，另一方面也节省了网络带宽。

表1-7 配置 IPv6 组播组成员快速离开

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
使能IPv6组播组成员快速离开功能	**mld fast-leave** [**group-policy** *acl6-number*]	缺省情况下，IPv6组播组成员快速离开功能处于关闭状态

1.5 配置MLD SSM Mapping

在 IPv6 SSM 网络中，由于各种可能的限制，某些接收者主机只能运行 MLDv1。为了向这些仅支持 MLDv1 的接收者主机提供 SSM 服务，可以在路由器上配置 MLD SSM Mapping 规则。

提示

由于 MLD SSM Mapping 不会对 MLDv2 的报告报文进行处理，因此为保证本网段内运行任意版本 MLD 的接收者主机都能得到 SSM 服务，建议在该网段的接口上运行 MLDv2。

1.5.1 配置准备

在配置 MLD SSM Mapping 规则之前，需完成以下任务：

- 配置任一 IPv6 单播路由协议，实现域内网络层互通
- 配置 MLD 基本功能

1.5.2 配置过程

表1-8 配置 MLD SSM Mapping

操作	命令	说明
进入系统视图	**system-view**	-
进入MLD视图	**mld** [**vpn-instance** *vpn-instance-name*]	-
配置MLD SSM Mapping规则	**ssm-mapping** *ipv6-source-address acl6-number*	缺省情况下，未配置MLD SSM Mapping规则

1.6 配置MLD代理

1.6.1 配置准备

在配置 MLD 代理之前，需完成以下任务：

- 配置任一 IPv6 单播路由协议，实现域内网络层互通

1.6.2 使能MLD代理功能

在设备朝向组播分发树树根方向的接口上使能了 MLD 代理功能之后，该设备就成为了 MLD 代理设备。

提示

- 如果在一个接口上同时使能 MLD 代理功能和 MLD 协议，MLD 协议将不会生效。在已使能 MLD 代理功能的接口上配置其它 MLD 命令时，只有 **mld version** 命令会生效。
- 如果在一台设备上同时使能 MLD 代理功能和 IPv6 组播路由协议（如 IPv6 PIM），IPv6 组播路由协议将不会生效。

表1-9 使能 MLD 代理功能

操作	命令	说明
进入系统视图	**system-view**	-
使能IPv6组播路由，并进入IPv6 MRIB视图	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	缺省情况下，IPv6组播路由处于关闭状态 本命令的详细介绍请参见“IP组播命令参考”中的“IPv6组播路由与转发”
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能MLD代理功能	**mld proxy enable**	缺省情况下，MLD代理功能处于关闭状态

1.6.3 配置非查询器转发功能

IPv6 组播数据通常只被查询器转发，非查询器不具备组播转发能力，这样可避免 IPv6 组播数据被重复转发。但如果 MLD 代理设备的下行接口未能当选查询器，应在该接口上使能非查询器转发功能，否则下游主机将无法收到 IPv6 组播数据。

提示

在共享网段内存在多台 MLD 代理设备的情况下，如果其中一台 MLD 代理设备的下行接口已当选为查询器，不应再在其它 MLD 代理设备的下行接口上使能非查询器转发功能，否则该网段将收到多份重复的 IPv6 组播数据。

表1-10 配置非查询器转发功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能非查询器转发功能	**mld proxy forwarding**	缺省情况下，非查询器转发功能处于关闭状态

1.6.4 配置MLD代理的负载分担功能

当在 MLD 代理设备的多个接口上使能了 MLD 代理功能时：

- 如果关闭了 MLD 代理的负载分担功能，则只有 IPv6 地址最大的接口会转发 IPv6 组播流量。
- 如果使能了 MLD 代理的负载分担功能，则可通过这些接口对 IPv6 组播流量按组进行负载分担。

表1-11 配置 MLD 代理的负载分担功能

操作	命令	说明
进入系统视图	**system-view**	-
进入MLD视图	**mld** [**vpn-instance** *vpn-instance-name*]	-
使能MLD代理的负载分担功能	**proxy multipath**	缺省情况下，MLD代理的负载分担功能处于关闭状态

1.7 MLD显示和维护

注意

执行 **reset mld group** 命令可能导致接收者中断 IPv6 组播信息的接收。

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 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 的统计信息。

表1-12 MLD 显示和维护

操作	命令
显示MLD组播组的信息	**display mld** [**vpn-instance** *vpn-instance-name*] **group** [*ipv6-group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**]
显示接口上MLD配置和运行信息	**display mld** [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**proxy**] [**verbose**]
显示MLD代理记录的IPv6组播组信息	**display mld** [**vpn-instance** *vpn-instance-name*] **proxy group** [*ipv6-group-address* | **interface** *interface-type interface-number*] [**verbose**]
显示MLD代理路由表的信息	**display mld** [**vpn-instance** *vpn-instance-name*] **proxy routing-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*]] * [**verbose**]
显示MLD SSM Mapping规则	**display mld** [**vpn-instance** *vpn-instance-name*] **ssm-mapping** *ipv6-group-address*
清除MLD组的动态加入记录	**reset mld** [**vpn-instance** *vpn-instance-name*] **group** { **all** | **interface** *interface-type interface-number* { **all** | *ipv6-group-address* [*prefix-length*] [*ipv6-source-address* [*prefix-length*]] } }

说明

reset mld group 命令只能清除动态加入记录，无法清除静态加入记录。

1.8 MLD典型配置举例

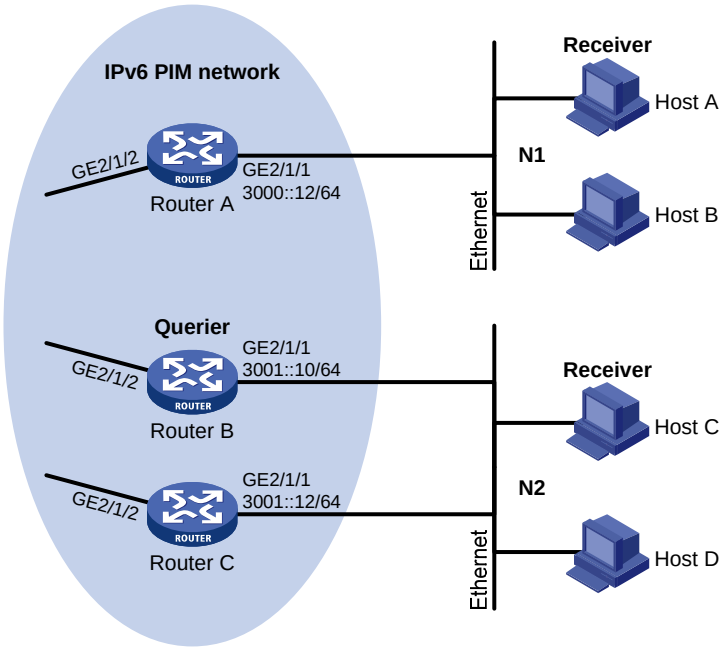
1.8.1 MLD基本功能配置举例

1. 组网需求

- 接收者通过组播方式接收视频点播信息，不同组织的接收者组成末梢网络 N1 和 N2，Host A 与 Host C 分别为 N1 和 N2 中的组播信息接收者。
- IPv6 PIM 网络中的 Router A 连接 N1，Router B 与 Router C 共同连接 N2。
- Router A 通过 GigabitEthernet2/1/1 连接 N1，通过 GigabitEthernet2/1/2 连接 IPv6 PIM 网络中的其它设备。
- Router B 与 Router C 分别通过各自的 GigabitEthernet2/1/1 连接 N2，并分别通过各自的 GigabitEthernet2/1/2 连接 IPv6 PIM 网络中的其它设备。
- Router A 与 N1 之间运行 MLDv1，Router A 为 MLD 查询器；Router B、Router C 与 N2 之间也分别运行 MLDv1，且由于 Router B 的接口 IPv6 地址较小，因此由其充当 MLD 查询器。
- 通过配置，使 N1 中的主机只能加入 IPv6 组播组 FF1E::101，而对 N2 中的主机则无任何限制。

2. 组网图

图1-5 MLD 基本功能配置组网图



3. 配置步骤

(1) 配置 IPv6 地址和 IPv6 单播路由协议

请按照 图 1-5 配置各接口的IPv6 地址和前缀长度，具体配置过程略。

配置 IPv6 PIM 网络内的各路由器之间采用 OSPFv3 协议进行互连，确保 IPv6 PIM 网络内部在网络层互通，并且各路由器之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IPv6 组播路由，并使能 IPv6 PIM-DM 和 MLD

在 Router A 上使能 IPv6 组播路由，在接口 GigabitEthernet2/1/2 上使能 IPv6 PIM-DM，并在接口 GigabitEthernet2/1/1 上使能 MLD。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mld enable
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ipv6 pim dm
[RouterA-GigabitEthernet2/1/2] quit
```

在 Router B 上使能 IPv6 组播路由，在接口 GigabitEthernet2/1/2 上使能 IPv6 PIM-DM，并在接口 GigabitEthernet2/1/1 上使能 MLD。

```
<RouterB> system-view
[RouterB] ipv6 multicast routing
[RouterB-mrib6] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mld enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] ipv6 pim dm
[RouterB-GigabitEthernet2/1/2] quit
```

在 Router C 上使能 IPv6 组播路由，在接口 GigabitEthernet2/1/2 上使能 IPv6 PIM-DM，并在接口 GigabitEthernet2/1/1 上使能 MLD。

```
<RouterC> system-view
[RouterC] ipv6 multicast routing
[RouterC-mrib6] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mld enable
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface gigabitethernet 2/1/2
[RouterC-GigabitEthernet2/1/2] ipv6 pim dm
[RouterC-GigabitEthernet2/1/2] quit
```

(3) 配置 IPv6 组播组过滤器

在 Router A 上限定接口 GigabitEthernet2/1/1 下的主机只能加入 IPv6 组播组 FF1E::101。

```
[RouterA] acl ipv6 number 2001
[RouterA-acl6-basic-2001] rule permit source ff1e::101 128
[RouterA-acl6-basic-2001] quit
[RouterA] interface gigabitethernet 2/1/1
```

```
[RouterA-GigabitEthernet2/1/1] mld group-policy 2001
[RouterA-GigabitEthernet2/1/1] quit
```

4. 验证配置

在 Router B 上显示接口 GigabitEthernet2/1/1 上 MLD 配置和运行的信息。

```
[RouterB] display mld interface gigabitethernet 2/1/1
 GigabitEthernet2/1/1(FE80::200:5EFF:FE66:5100):
   MLD is enabled.
   MLD version: 1
   Query interval for MLD: 125s
   Other querier present time for MLD: 255s
   Maximum query response time for MLD: 10s
   Querier for MLD: FE80::200:5EFF:FE66:5100 (this router)
  MLD groups reported in total: 1
```

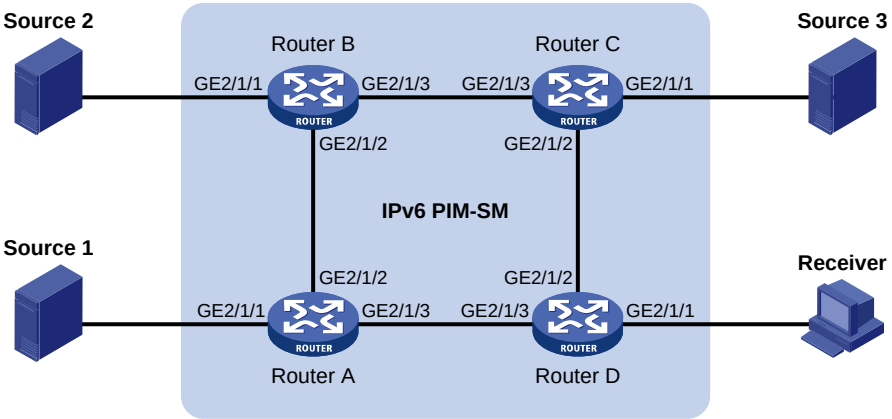
1.8.2 MLD SSM Mapping配置举例

1. 组网需求

- IPv6 PIM-SM 网络中同时采用 ASM 和 SSM 方式提供 IPv6 组播服务，将 Router D 的接口 GigabitEthernet2/1/3 配置为 C-BSR 和 C-RP，IPv6 SSM 组播组的范围为 FF3E::/64。
- Router D 的接口 GigabitEthernet2/1/1 上运行 MLDv2，接收者主机上运行 MLDv1，且不能升级至 MLDv2，因此该主机在加入 IPv6 组播组时无法指定 IPv6 组播源。
- Source 1、Source 2 和 Source 3 都向 IPv6 SSM 组范围内的组播组发送 IPv6 组播数据，要求通过在 Router D 上配置 MLD SSM Mapping 规则，使接收者主机只能接收来自 Source 1 和 Source 3 的 IPv6 组播数据。

2. 组网图

图1-6 MLD SSM Mapping 配置组网图



设备	接口	IPv6地址	设备	接口	IPv6地址
Source 1	-	1001::1/64	Source 3	-	3001::1/64
Source 2	-	2001::1/64	Receiver	-	4001::1/64
Router A	GE2/1/1	1001::2/64	Router C	GE2/1/1	3001::2/64
	GE2/1/2	1002::1/64		GE2/1/2	3002::1/64
	GE2/1/3	1003::1/64		GE2/1/3	2002::2/64
Router B	GE2/1/1	2001::2/64	Router D	GE2/1/1	4001::2/64
	GE2/1/2	1002::2/64		GE2/1/2	3002::2/64
	GE2/1/3	2002::1/64		GE2/1/3	1003::2/64

3. 配置步骤

(1) 配置 IPv6 地址和 IPv6 单播路由协议

请按照 图 1-6 配置各接口的IPv6 地址和前缀长度，具体配置过程略。

配置 IPv6 PIM-SM 域内的各路由器之间采用 OSPFv3 协议进行互连，确保 IPv6 PIM-SM 域内部在网络层互通，并且各路由器之间能够借助 IPv6 单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IPv6 组播路由，并使能 IPv6 PIM-SM 和 MLD

在 Router D 上使能 IPv6 组播路由，在主机侧接口 GigabitEthernet2/1/1 上使能 MLD，配置 MLD 版本为 2；并在其它接口上使能 IPv6 PIM-SM。

```
<RouterD> system-view
[RouterD] ipv6 multicast routing
[RouterD-mrib6] quit
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] mld enable
[RouterD-GigabitEthernet2/1/1] mld version 2
[RouterD-GigabitEthernet2/1/1] quit
[RouterD] interface gigabitethernet 2/1/2
[RouterD-GigabitEthernet2/1/2] ipv6 pim sm
[RouterD-GigabitEthernet2/1/2] quit
[RouterD] interface gigabitethernet 2/1/3
[RouterD-GigabitEthernet2/1/3] ipv6 pim sm
[RouterD-GigabitEthernet2/1/3] quit
```

在 Router A 上使能 IPv6 组播路由，并在各接口上使能 IPv6 PIM-SM。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ipv6 pim sm
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ipv6 pim sm
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] interface gigabitethernet 2/1/3
[RouterA-GigabitEthernet2/1/3] ipv6 pim sm
[RouterA-GigabitEthernet2/1/3] quit
```

Router B 和 Router C 的配置与 Router A 相似，配置过程略。

(3) 配置 C-BSR 和 C-RP

在 Router D 上配置 C-BSR 和 C-RP 的位置。

```
[RouterD] ipv6 pim
[RouterD-pim6] c-bsr 1003::2
[RouterD-pim6] c-rp 1003::2
[RouterD-pim6] quit
```

(4) 配置 IPv6 SSM 组播组的地址范围

在 Router D 上配置 IPv6 SSM 组播组的地址范围为 FF3E::/64。

```
[RouterD] acl ipv6 number 2000
[RouterD-acl6-basic-2000] rule permit source ff3e:: 64
[RouterD-acl6-basic-2000] quit
[RouterD] ipv6 pim
[RouterD-pim6] ssm-policy 2000
[RouterD-pim6] quit
```

Router A、Router B 和 Router C 的配置与 Router D 相似，配置过程略。

(5) 配置 MLD SSM Mapping 规则

在 Router D 上配置 MLD SSM Mapping 规则。

```
[RouterD] mld
[RouterD-mld] ssm-mapping 1001::1 2000
[RouterD-mld] ssm-mapping 3001::1 2000
[RouterD-mld] quit
```

4. 验证配置

显示 Router D 上 IPv6 组播组 FF3E::101 对应的 MLD SSM Mapping 规则。

```
[RouterD] display mld ssm-mapping ff3e::101
 Group: FF3E::101
 Source list:
        1001::1
        3001::1
```

显示 Router D 上公网实例中依据 MLD SSM Mapping 规则创建的 MLD 组播组信息。

```
[RouterD] display mld group
MLD groups in total: 1
 GigabitEthernet2/1/1(FE80::101):
  MLD groups reported in total: 1
   Group address: FF3E::101
    Last reporter: FE80::1
    Uptime: 00:02:04
    Expires: Off
```

显示 Router D 上公网实例 IPv6 PIM 路由表的内容。

```
[RouterD] display ipv6 pim routing-table
 Total 0 (*, G) entry; 2 (S, G) entry

 (1001::1, FF3E::101)
     RP: 1003::2
     Protocol: pim-ssm, Flag:
     UpTime: 00:13:25
     Upstream interface: GigabitEthernet2/1/3
         Upstream neighbor: 1003::1
         RPF prime neighbor: 1003::1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/1/1
             Protocol: mld, UpTime: 00:13:25, Expires: -

 (3001::1, FF3E::101)
```

```
RP: 1003::2
Protocol: pim-ssm, Flag:
UpTime: 00:13:25
Upstream interface: GigabitEthernet2/1/2
    Upstream neighbor: 3002::1
    RPF prime neighbor: 3002::1
Downstream interface(s) information:
Total number of downstreams: 1
    1: GigabitEthernet2/1/1
        Protocol: mld, UpTime: 00:13:25, Expires: -
```

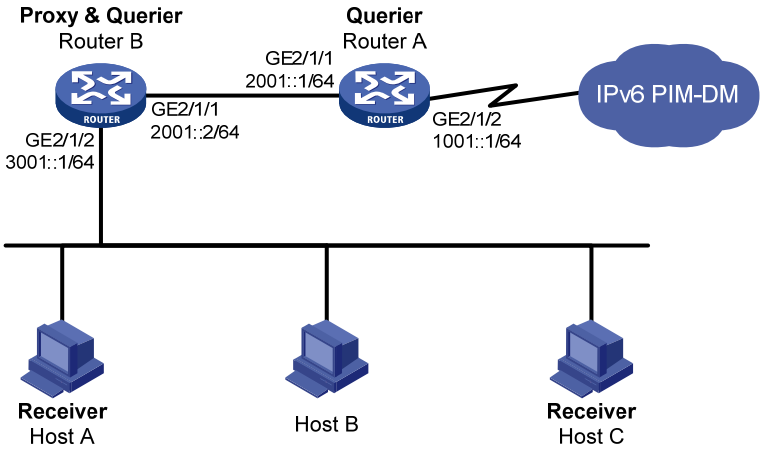
1.8.3 MLD代理配置举例

1. 组网需求

- 核心网络中运行 IPv6 PIM-DM，末梢网络中的接收者 Host A 和 Host C 通过 IPv6 组播组 FF1E::1 点播视频节目。
- 要求通过在 Router B 上配置 MLD 代理，使其在不运行 IPv6 PIM-DM 的情况下实现组成员关系的维护和 IPv6 组播数据的正常转发。

2. 组网图

图1-7 MLD 代理配置组网图



3. 配置步骤

(1) 配置 IPv6 地址

请按照 图 1-7 配置各接口的IPv6 地址和前缀长度，具体配置过程略。

(2) 使能 IPv6 组播路由，并使能 IPv6 PIM-DM、MLD 和 MLD 代理

在 Router A 上使能 IPv6 组播路由，在接口 GigabitEthernet2/1/2 上使能 IPv6 PIM-DM，并在接口 GigabitEthernet2/1/1 上使能 MLD。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 2/0/2
[RouterA-GigabitEthernet2/1/2] ipv6 pim dm
```

```
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mld enable
[RouterA-GigabitEthernet2/1/1] quit
```

在 Router B 上使能 IPv6 组播路由，在接口 GigabitEthernet2/1/1 上使能 MLD 代理，并在接口 GigabitEthernet2/1/2 上使能 MLD。

```
<RouterB> system-view
[RouterB] ipv6 multicast routing
[RouterB-mrib6] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mld proxy enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] mld enable
[RouterB-GigabitEthernet2/1/2] quit
```

4. 验证配置

在 Router B 上显示 MLD 代理记录的所有 IPv6 组播组信息。

```
[RouterB] display mld proxy group
MLD proxy group records in total: 1
 GigabitEthernet2/1/1(FE80::16:1):
  MLD proxy group records in total: 1
   Group address: FF1E::1
    Member state: Delay
    Expires: 00:00:02
```

1.9 常见配置错误举例

1.9.1 接收者侧路由器上无组成员信息

1. 故障现象

当某主机发送了加入 IPv6 组播组 G 的报文后，离该主机最近的路由器上却没有 IPv6 组播组 G 的组成员信息。

2. 分析

- 组网、接口连线的正确与否以及接口的协议层是否 up 将直接影响 IPv6 组播组成员信息的生成；
- 在路由器上必须使能 IPv6 组播路由，在连接主机的接口上必须使能 MLD；
- 如果路由器接口上运行的 MLD 版本比主机的低，那么路由器将无法识别主机发来的较高版本的 MLD 报告报文；
- 如果在接口上使用命令 **mld group-policy** 对加入 IPv6 组播组 G 进行了限制后，该接口将不再接收未通过过滤的那些要求加入 IPv6 组播组 G 的报文。

3. 处理过程

(1) 检查组网是否正确，接口间的连线是否正确，以及接口状态是否正常，是否配置了正确的 IPv6 地址。通过命令 **display mld interface** 查看接口信息。若无接口信息输出，说明接口状态异

常，原因通常是接口上配置了 **shutdown** 命令，或者接口连线不正确，或者接口上没有配置正确的 IPv6 地址。

(2) 检查是否使能了 IPv6 组播路由。通过命令 **display current-configuration** 查看是否配置了命令 **ipv6 multicast routing**。若缺少该配置，则需要在系统视图下执行命令 **ipv6 multicast routing** 使能 IPv6 组播路由，同时也需要在相应接口上使能 MLD。

(3) 检查接口上运行的 MLD 版本。通过命令 **display mld interface** 来检查接口上运行的 MLD 版本是否低于主机所使用的版本。

(4) 检查接口上是否配置了 IPv6 ACL 规则来限制主机加入 IPv6 组播组 G。通过命令 **display current-configuration interface** 观察是否配置了 **mld group-policy** 命令。如果配置的 IPv6 ACL 规则对加入 IPv6 组播组 G 进行了限制，则需要修改该 IPv6 ACL 规则，允许接受 IPv6 组播组 G 的报告报文。

1.9.2 同一网段各路由器上组成员关系不一致

1. 故障现象

在同一网段的不同 MLD 路由器上，各自维护的组成员关系不一致。

2. 分析

- 运行 MLD 的路由器为每个接口维护多个参数，各参数之间相互影响，非常复杂。如果同一网段路由器的 MLD 接口参数配置不一致，必然导致组成员关系的混乱。
- 另外，MLD 目前有 2 个版本，版本不同的 MLD 路由器与主机之间虽然可以部分兼容，但是连接在同一网段的所有路由器必须运行相同版本的 MLD。如果同一网段路由器的 MLD 版本不一致，也将导致 MLD 组成员关系的混乱。

3. 处理过程

(1) 检查 MLD 配置。通过命令 **display current-configuration** 观察接口上 MLD 的配置信息。

(2) 在同一网段的所有路由器上执行命令 **display mld interface** 来检查 MLD 相关定时器的参数，确保配置一致。

(3) 通过命令 **display mld interface** 来检查各路由器上运行的 MLD 版本是否一致。

目 录

1 IPv6 PIM

1.1 IPv6 PIM简介

IPv6 PIM（IPv6 Protocol Independent Multicast，IPv6 协议无关组播）协议利用 IPv6 单播静态路由或者任意 IPv6 单播路由协议（包括 RIPng、OSPFv3、IPv6 IS-IS、IPv6 BGP 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。有关 RPF 的详细介绍，请参见“IP 组播配置指导”中的“IPv6 组播路由与转发”。

根据实现机制的不同，IPv6 PIM 分为以下几种类型：

- IPv6 PIM-DM（IPv6 Protocol Independent Multicast-Dense Mode，IPv6 协议无关组播—密集模式）
- IPv6 PIM-SM（IPv6 Protocol Independent Multicast-Sparse Mode，IPv6 协议无关组播—稀疏模式）
- IPv6 BIDIR-PIM（IPv6 Bidirectional Protocol Independent Multicast，IPv6 双向协议无关组播，简称 IPv6 双向 PIM）
- IPv6 PIM-SSM（IPv6 Protocol Independent Multicast Source-Specific Multicast，IPv6 协议无关组播－指定源组播）

为了描述方便，本文中把由支持 IPv6 PIM 协议的组播路由器所组成的网络简称为“IPv6 PIM 域”。

1.1.1 IPv6 PIM-DM简介

IPv6 PIM-DM 属于密集模式的 IPv6 组播路由协议，使用“推（Push）模式”传送 IPv6 组播数据，通常适用于 IPv6 组播组成员相对比较密集的小型网络，其基本原理如下：

- IPv6 PIM-DM 假设网络中的每个子网都存在至少一个 IPv6 组播组成员，因此 IPv6 组播数据将被扩散（Flooding）到网络中的所有节点。然后，IPv6 PIM-DM 对没有 IPv6 组播数据转发的分支进行剪枝（Prune），只保留包含接收者的分支。这种“扩散—剪枝”现象周期性地发生，被剪枝的分支也可以周期性地恢复成转发状态。
- 当被剪枝分支的节点上出现了 IPv6 组播组的成员时，为了减少该节点恢复成转发状态所需的时间，IPv6 PIM-DM 使用嫁接（Graft）机制主动恢复其对 IPv6 组播数据的转发。

一般说来，密集模式下数据包的转发路径是有源树（Source Tree），即以 IPv6 组播源为“根”、IPv6 组播组成员为“叶子”的一棵转发树。由于有源树使用的是从 IPv6 组播源到接收者的最短路径，因此也称为 SPT（Shortest Path Tree，最短路径树）。

IPv6 PIM-DM 的工作机制如下：

1. 邻居发现

在 IPv6 PIM 域中，路由器上每个运行了 IPv6 PIM 协议的接口通过定期向本网段的所有 IPv6 PIM 路由器组播 IPv6 PIM Hello 报文（以下简称 Hello 报文），以发现 IPv6 PIM 邻居，维护各路由器之间的 IPv6 PIM 邻居关系，从而构建和维护 SPT。

2. 构建SPT

构建 SPT 的过程也就是“扩散—剪枝”的过程：

(1) 在 IPv6 PIM-DM 域中，IPv6 组播源 S 向 IPv6 组播组 G 发送 IPv6 组播报文时，首先对 IPv6 组播报文进行扩散：路由器对该报文的 RPF 检查通过后，便创建一个（S，G）表项，并将该报文向网络中的所有下游节点转发。经过扩散，IPv6 PIM-DM 域内的每个路由器上都会创建（S，G）表项。

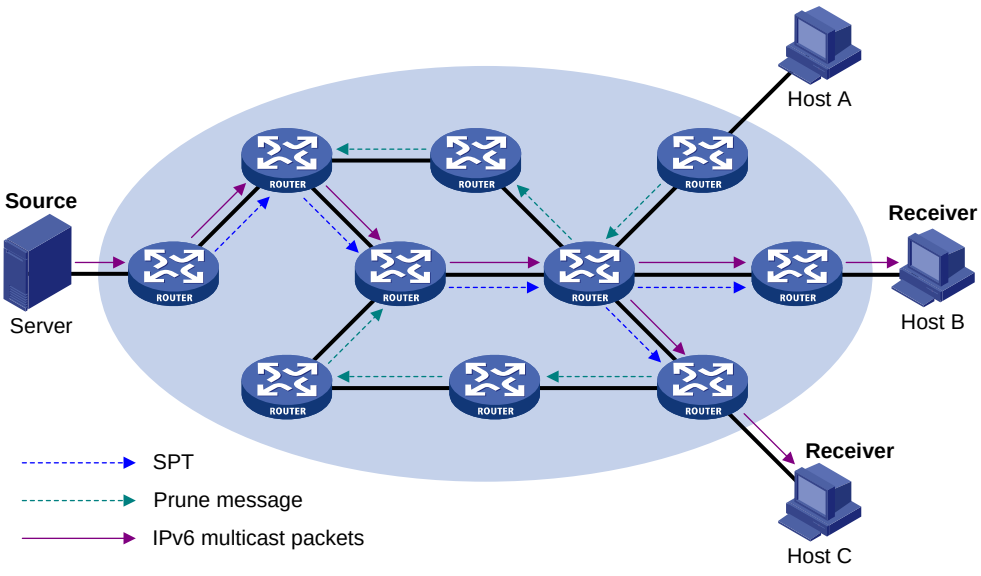
(2) 然后对那些下游没有接收者的节点进行剪枝：由没有接收者的下游节点向上游节点发剪枝报文（Prune Message），以通知上游节点将相应的接口从其组播转发表项（S，G）所对应的出接口列表中删除，并不再转发该 IPv6 组播组的报文至该节点。

说明

（S，G）表项包括 IPv6 组播源的地址 S、IPv6 组播组的地址 G、出接口列表和入接口等。

剪枝过程最先由“叶子”路由器发起，如 图 1-1 所示，由没有接收者（Receiver）的接口主动发起剪枝，并一直持续到IPv6 PIM-DM域中只剩下必要的分支，这些分支共同构成了SPT。

图1-1 IPv6 PIM-DM 中构建 SPT 示意图



“扩散—剪枝”的过程是周期性发生的。各个被剪枝的节点提供超时机制，当剪枝超时后便重新开始这一过程。

3. 嫁接

当被剪枝的节点上出现了 IPv6 组播组的成员时，为了减少该节点恢复成转发状态所需的时间，IPv6 PIM-DM 使用嫁接机制主动恢复其对 IPv6 组播数据的转发，过程如下：

(1) 需要恢复接收 IPv6 组播数据的节点向其上游节点发送嫁接报文（Graft Message）以申请重新加入到 SPT 中；

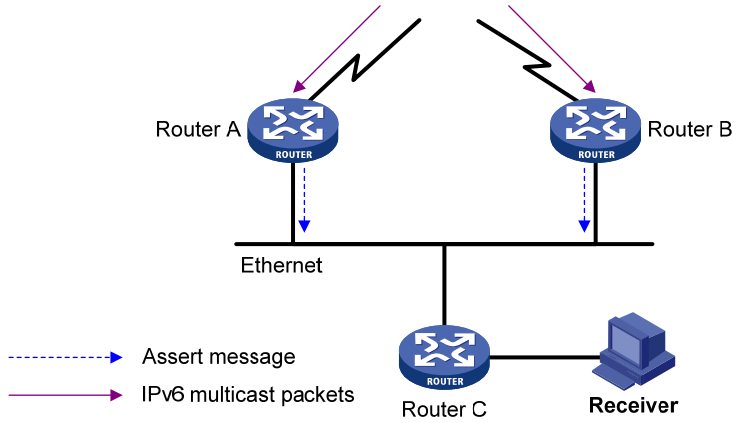
(2) 当上游节点收到该报文后恢复该下游节点的转发状态，并向其回应一个嫁接应答报文（Graft-Ack Message）以进行确认；

(3) 如果发送嫁接报文的下游节点没有收到来自其上游节点的嫁接应答报文，将重新发送嫁接报文直到被确认为止。

4. 断言

在一个网段内如果存在多台组播路由器，则相同的 IPv6 组播报文可能会被重复发送到该网段。为了避免出现这种情况，就需要通过断言（Assert）机制来选定唯一的 IPv6 组播数据转发者。

图1-2 Assert 机制示意图



如 图 1-2 所示，当Router A和Router B从上游节点收到（S，G）的IPv6 组播报文后，都会向本地网段转发该报文，于是处于下游的节点Router C就会收到两份相同的IPv6 组播报文，Router A和Router B也会从各自的下游接口收到对方转发来的该IPv6 组播报文。此时，Router A和Router B会通过其下游接口向本网段的所有IPv6 PIM路由器以组播方式发送断言报文（Assert Message），该报文中携带有以下信息：IPv6 组播源地址S、IPv6 组播地址G、到IPv6 组播源的IPv6 单播路由/IPv6 MBGP路由/IPv6 组播静态路由的优先级和度量值。通过一定的规则对这些参数进行比较后，Router A和Router B中的获胜者将成为（S，G）IPv6 组播报文在本网段的转发者，比较规则如下：

(1) 到 IPv6 组播源的优先级较高者获胜；

(2) 如果到 IPv6 组播源的优先级相等，那么到 IPv6 组播源的度量值较小者获胜；

(3) 如果到 IPv6 组播源的度量值也相等，则下游接口 IPv6 链路本地地址较大者获胜。

1.1.2 IPv6 PIM-SM简介

IPv6 PIM-DM 使用以“扩散—剪枝”方式构建的 SPT 来传送 IPv6 组播数据。尽管 SPT 的路径最短，但是其建立的过程效率较低，并不适合大中型网络。而 IPv6 PIM-SM 则属于稀疏模式的 IPv6 组播路由协议，使用“拉（Pull）模式”传送 IPv6 组播数据，通常适用于 IPv6 组播组成员分布相对分散、范围较广的大中型网络，其基本原理如下：

- IPv6 PIM-SM 假设所有主机都不需要接收 IPv6 组播数据，只向明确提出需要 IPv6 组播数据的主机转发。IPv6 PIM-SM 实现组播转发的核心任务就是构造并维护 RPT（Rendezvous Point

Tree，共享树），RPT 选择 IPv6 PIM 域中某台路由器作为公用的根节点 RP（Rendezvous Point，汇集点），IPv6 组播数据通过 RP 沿着 RPT 转发给接收者；

- 组播源侧 DR（Designated Router，指定路由器）向某 IPv6 组播组对应的 RP 发送加入报文，该报文被逐跳送达 RP，所经过的路径就形成了 RPT 的分支；
- IPv6 组播源如果要向某 IPv6 组播组发送 IPv6 组播数据，首先由 IPv6 组播源侧 DR 负责向 RP 进行注册，把注册报文（Register Message）通过单播方式发送给 RP，该报文到达 RP 后触发建立 SPT。之后 IPv6 组播源把 IPv6 组播数据沿着 SPT 发向 RP，当 IPv6 组播数据到达 RP 后，被复制并沿着 RPT 发送给接收者。

说明

复制仅发生在分发树的分支处，这个过程能够自动重复直到数据包最终到达接收者。

IPv6 PIM-SM 的工作机制如下：

1. 邻居发现

IPv6 PIM-SM使用与IPv6 PIM-DM类似的邻居发现机制，具体请参见“1.1.1 1. 邻居发现”一节。

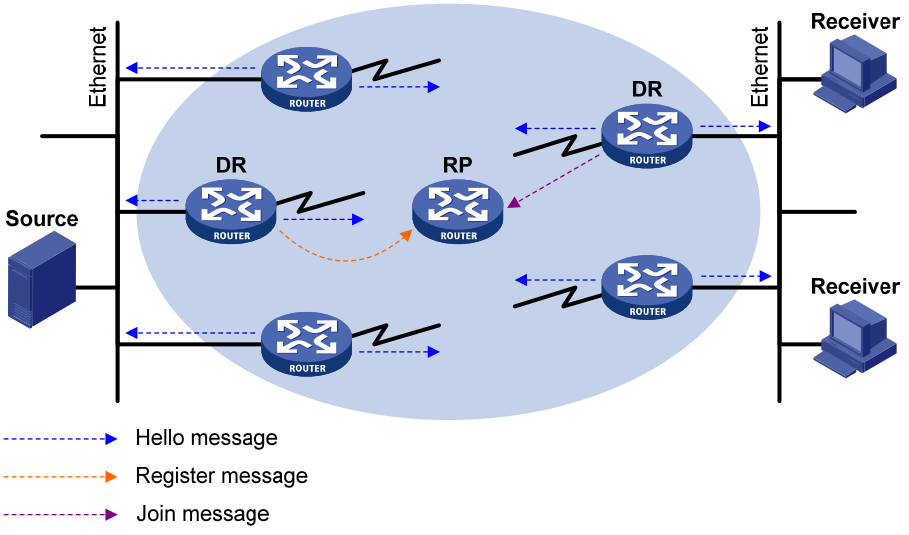
2. DR选举

DR 是共享网络（如以太网）中 IPv6 组播数据的唯一转发者。无论是与 IPv6 组播源相连的网络，还是与接收者相连的网络，都需要选举 DR。接收者侧的 DR 负责向 RP 发送加入报文；IPv6 组播源侧的 DR 负责向 RP 发送注册报文。

提示

在充当接收者侧 DR 的设备上必须使能 MLD，否则连接在该 DR 上的接收者将不能通过该 DR 加入 IPv6 组播组。有关 MLD 的详细介绍，请参见“IP 组播配置指导”中的“MLD”。

图1-3 DR 选举示意图



如 图 1-3 所示，DR的选举过程如下：

(1) 共享网络上的各路由器相互之间发送 Hello 报文（携带有竞选 DR 优先级的参数），拥有最高优先级的路由器将成为 DR；

(2) 如果优先级相同，或者网络中至少有一台路由器不支持在 Hello 报文中携带竞选 DR 优先级的参数，则根据各路由器的 IPv6 链路本地地址大小来竞选 DR，IPv6 链路本地地址最大的路由器将成为 DR。

如果 DR 出现故障，将导致其 IPv6 PIM 邻居可达状态定时器超时，其余路由器将触发新的 DR 选举过程。

3. RP发现

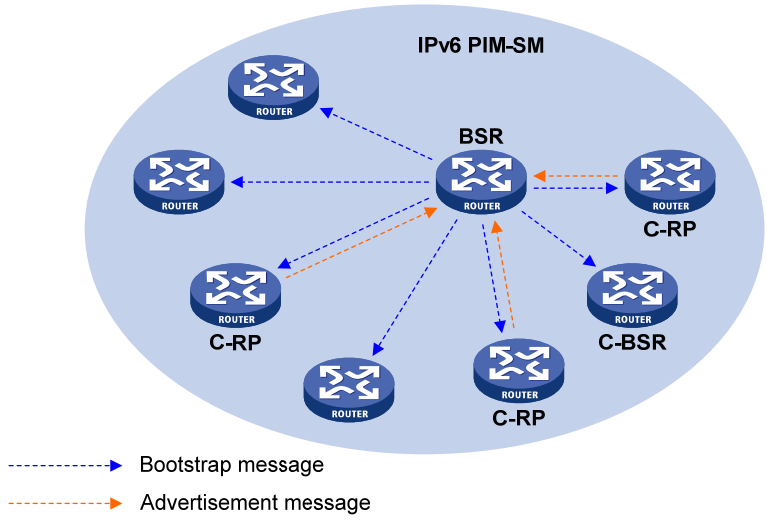
RP 是 IPv6 PIM-SM 域中的核心设备。在结构简单的小型网络中，IPv6 组播信息量少，整个网络仅依靠一个 RP 进行 IPv6 组播信息的转发即可，此时可以在 IPv6 PIM-SM 域中的各路由器上静态指定 RP 的位置；但是在更多的情况下，IPv6 PIM-SM 域的规模都很大，通过 RP 转发的 IPv6 组播信息量巨大。为了缓解 RP 的负担并优化 RPT 的拓扑结构，可以在 IPv6 PIM-SM 域中配置多个 C-RP（Candidate-RP，候选 RP），通过自举机制来动态选举 RP，使不同的 RP 服务于不同的组播组，此时需要配置 BSR（Bootstrap Router，自举路由器）。BSR 是 IPv6 PIM-SM 域中的管理核心，一个 IPv6 PIM-SM 域内只能有一个 BSR，但可以配置多个 C-BSR（Candidate-BSR，候选 BSR）。这样，一旦 BSR 发生故障，其余 C-BSR 能够通过自动选举产生新的 BSR，从而确保业务免受中断。

说明

- 一个 RP 可以同时服务于多个 IPv6 组播组，但一个 IPv6 组播组只能唯一对应一个 RP。
- 一台设备可以同时充当 C-RP 和 C-BSR。

如 图 1-4 所示，BSR负责收集网络中由C-RP发来的宣告报文（Advertisement Message），该报文中携带有C-RP的地址和优先级以及其服务的IPv6 组范围，BSR将这些信息汇总为RP-Set（RP集，即IPv6 组播组与RP的映射关系数据库），封装在自举报文（Bootstrap Message，BSM）中并发布到整个IPv6 PIM-SM域。

图1-4 RP 与 BSR 信息交互示意图



网络中的各路由器将依据 RP-Set 提供的信息，使用相同的规则从众多 C-RP 中为特定 IPv6 组播组选择其对应的 RP，具体规则如下：

(1) 首先比较 C-RP 所服务的 IPv6 组范围，所服务的 IPv6 组范围较小者获胜。

(2) 若服务的 IPv6 组范围相同，再比较 C-RP 的优先级，优先级较高者获胜。

(3) 若优先级也相同，再使用哈希（Hash）函数计算哈希值，哈希值较大者获胜。

(4) 若哈希值也相同，则 C-RP 的 IPv6 地址较大者获胜。

4. 嵌入式RP

通过嵌入式 RP（Embedded RP）机制可以从 IPv6 组播地址中解析出 RP 的地址，从而实现 IPv6 组播组到 RP 的映射，以取代静态配置的 RP 或由 BSR 机制动态计算出来的 RP，DR 不再需要预先知道 RP 的信息，只需对组播报文进行分析即可知道 RP 的地址。其工作原理如下：

- 接收者侧：

(1) 接收者主机发送 MLD 报告报文声明加入某 IPv6 组播组；

(2) 接收者侧的 DR 提取内嵌在 IPv6 组播地址中的 RP 地址，并向该 RP 发送加入报文（Join Message）。

- IPv6 组播源侧：

(1) IPv6 组播源要向某 IPv6 组播组发送 IPv6 组播数据；

(2) IPv6 组播源侧的 DR 提取内嵌在 IPv6 组播地址中的 RP 地址，并向该 RP 发送注册报文。

5. Anycast-RP

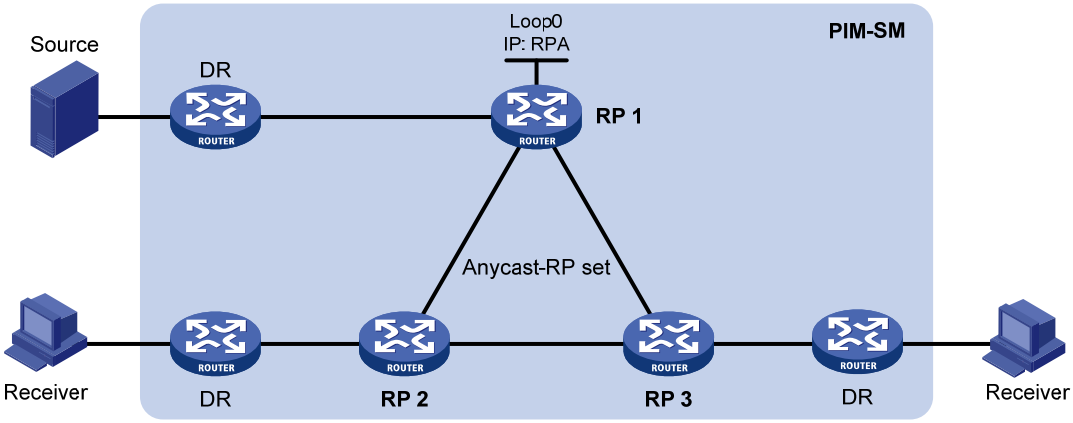
IPv6 PIM-SM 要求每个 IPv6 组播组只能有一个激活的 RP，因此当某 RP 失效时，可能导致其对应 IPv6 组播组的流量中断。Anycast-RP 机制通过为同一 IPv6 组播组设置具有相同地址的多个 RP，IPv6 组播源和接收者各自就近选择 RP 进行注册或加入，这些 RP 之间则进行 IPv6 组播源信息的同步，从而实现了 RP 间的冗余备份。Anycast-RP 具有以下优点：

- RP 路径最优：IPv6 组播源向距离最近的 RP 进行注册，建立路径最优的 SPT；接收者向距离最近的 RP 发起加入，建立路径最优的 RPT。

- RP 冗余备份：当某 RP 失效后，原先在该 RP 上注册或加入的 IPv6 组播源或接收者会自动选择就近的 RP 进行注册或加入，从而实现了 RP 间的冗余备份。

由服务于同一IPv6 组播组的多个RP组成的集合称为Anycast-RP集，这些RP则称为Anycast-RP成员，各成员的地址称为Anycast-RP成员地址，而Anycast-RP集对外统一发布的地址则称为Anycast-RP地址。如 图 1-5 所示，一个Anycast-RP集中包含RP 1、RP 2 和RP 3 三个成员，Anycast-RP地址为RPA。

图1-5 Anycast-RP 示意图



Anycast-RP 的工作过程如下：

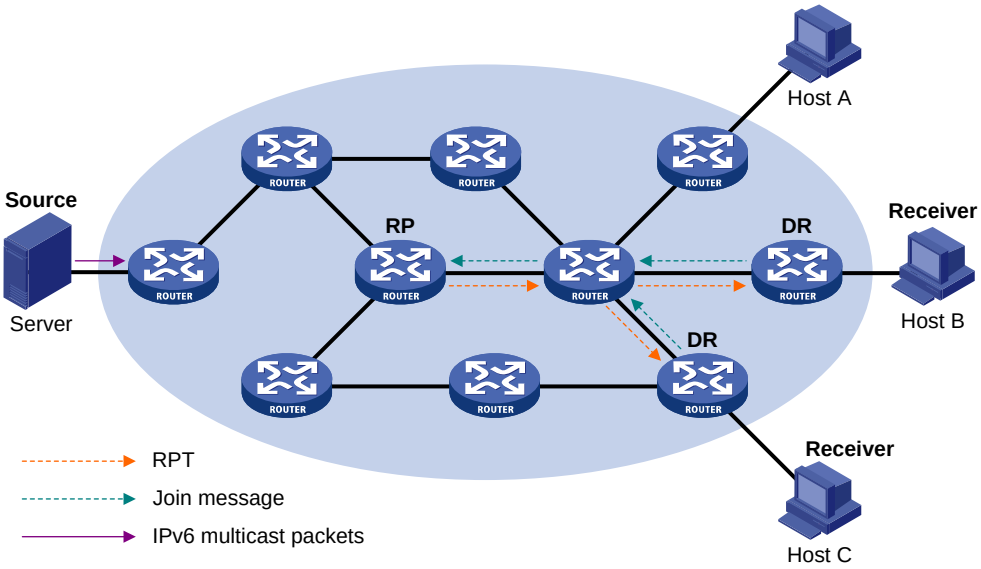
(1) RP 1 收到一个目的地址为 RPA 的注册报文，发现其源地址不是其它成员（RP 2 或 RP 3）的地址，于是认为此报文由 DR 发来。然后 RP 1 将该报文的源地址改为自己的地址后发送给所有其它成员（RP 2 和 RP 3）。如果一台设备既是 DR 也是 RP，则相当于收到自己发送的注册报文，也要向所有其它成员转发。

(2) RP 2 和 RP 3 收到 RP 1 发来的注册报文后，发现其源地址是 Anycast-RP 集的成员地址，于是不再向外转发。

由此可见，RP 接收注册报文的原有处理没有任何改变，唯一的变化就是满足条件的 RP 要向同一 Anycast-RP 集内的其它成员转发注册报文，以实现 IPv6 组播源信息的共享。

6. 构建RPT

图1-6 IPv6 PIM-SM 中构建 RPT 示意图



如 图 1-6 所示，RPT的构建过程如下：

(1) 当接收者加入一个 IPv6 组播组 G 时，先通过 MLD 报文通知与其直连的 DR；

(2) DR 掌握了 IPv6 组播组 G 的接收者的信息后，向该组所对应的 RP 方向逐跳发送加入报文；

(3) 从 DR 到 RP 所经过的路由器就形成了 RPT 的分支，这些路由器都在其转发表中生成了（*，G）表项，这里的“*”表示来自任意 IPv6 组播源。RPT 以 RP 为根，以 DR 为叶子。

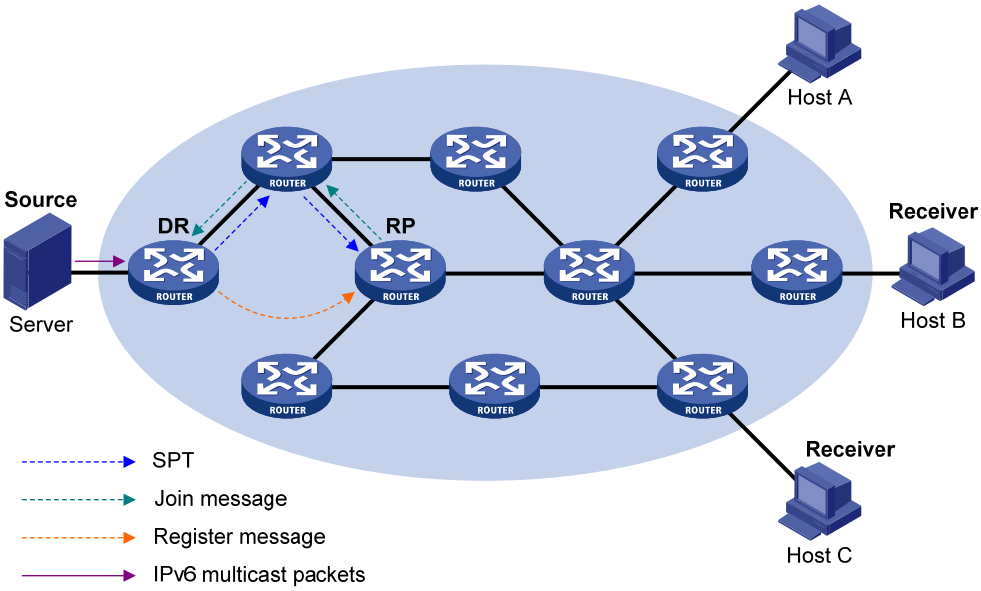
当发往 IPv6 组播组 G 的 IPv6 组播数据流经 RP 时，数据就会沿着已建立好的 RPT 到达 DR，进而到达接收者。

当某接收者对 IPv6 组播组 G 的信息不再感兴趣时，与其直连的 DR 会逆着 RPT 向该组的 RP 方向逐跳发送剪枝报文；上游节点收到该报文后在其出接口列表中删除与下游节点相连的接口，并检查自己是否拥有该 IPv6 组播组的接收者，如果没有则继续向其上游转发该剪枝报文。

7. IPv6 组播源注册

IPv6 组播源注册的目的是向 RP 通知 IPv6 组播源的存在。

图1-7 IPv6 组播源注册示意图



如 图 1-7 所示，IPv6 组播源向RP注册的过程如下：

(1) 当 IPv6 组播源 S 向 IPv6 组播组 G 发送了一个 IPv6 组播报文时，与 IPv6 组播源直连的 DR 在收到该报文后，就将其封装成注册报文，并通过单播方式发送给相应的 RP；

(2) 当 RP 收到该报文后，一方面解封装注册报文并将封装在其中的 IPv6 组播报文沿着 RPT 转发给接收者，另一方面向 IPv6 组播源方向逐跳发送（S，G）加入报文。这样，从 RP 到 IPv6 组播源所经过的路由器就形成了 SPT 的分支，这些路由器都在其转发表中生成了（S，G）表项。

(3) IPv6 组播源发出的 IPv6 组播数据沿着已建立好的 SPT 到达 RP，然后由 RP 把 IPv6 组播数据沿着 RPT 向接收者进行转发。当 RP 收到沿着 SPT 转发来的 IPv6 组播数据后，通过单播方式向与 IPv6 组播源直连的 DR 发送注册停止报文（Register-Stop Message），IPv6 组播源注册过程结束。

说明

上述描述中假定允许 RP 发起 SPT 切换，否则 IPv6 组播源侧 DR 将一直用注册报文封装 IPv6 组播报文，注册过程不会结束。

---

8. SPT切换

在 IPv6 PIM-SM 域中，一个 IPv6 组播组唯一对应一个 RP 和一棵 RPT。在 SPT 切换前，所有发往该组的 IPv6 组播报文都必须先由 IPv6 组播源侧 DR 封装在注册报文中发往 RP，由 RP 解封装后再沿 RPT 分发给接收者侧的 DR，RP 是所有 IPv6 组播数据必经的中转站。这个过程存在以下三个问题：

- IPv6 组播源侧的 DR 和 RP 必须对 IPv6 组播数据进行繁琐的封装/解封装处理。
- IPv6 组播数据的转发路径不一定是从 IPv6 组播源到接收者的最短路径。
- 当 IPv6 组播流量变大时，RP 负担增大，容易引发故障。

为了解决上述问题，当 IPv6 组播数据的转发速率超过阈值时，IPv6 PIM-SM 允许由 RP 或接收者侧的 DR 发起 SPT 切换：

(1) RP 发起的 SPT 切换

RP 周期性地检测 IPv6 组播数据（S，G）的转发速率，一旦发现其超过阈值，立即向 IPv6 组播源方向发送（S，G）加入报文，建立 RP 到 IPv6 组播源的 SPT 分支，后续的 IPv6 组播报文都直接沿该分支到达 RP。

由RP发起的SPT切换的详细过程，请参见“1.1.2 7. IPv6 组播源注册”一节。

(2) 接收者侧 DR 发起的 SPT 切换

接收者侧 DR 周期性地检测 IPv6 组播数据（S，G）的转发速率，一旦发现其超过阈值，立即发起 SPT 切换，过程如下：

- 首先，接收者侧 DR 向 IPv6 组播源方向逐跳发送（S，G）加入报文，沿途经过的所有路由器在其转发表中都生成了（S，G）表项，从而建立了 SPT 分支；
- 随后，当 IPv6 组播数据沿 SPT 到达 RPT 与 SPT 分叉的路由器时，该路由器开始丢弃沿 RPT 到达的 IPv6 组播数据，同时向 RP 逐跳发送含 RP 位的剪枝报文，RP 收到该报文后继续向 IPv6 组播源方向发送剪枝报文（假设此时只有这一个接收者），从而完成了 SPT 切换；
- 最终，IPv6 组播数据将沿 SPT 从 IPv6 组播源到达到接收者。

通过 SPT 切换，IPv6 PIM-SM 能够以比 IPv6 PIM-DM 更经济的方式建立 SPT。

9. 断言

IPv6 PIM-SM使用与IPv6 PIM-DM类似的断言机制，具体请参见“4. 断言”一节。

1.1.3 IPv6 双向PIM简介

在某些组网应用（譬如多方电视电话会议）中，同时存在多个接收者和多个 IPv6 组播源，在这种情况下，如果使用传统的 IPv6 PIM-DM 或 IPv6 PIM-SM 按 SPT 转发 IPv6 组播数据，需在每台路由器上针对每个 IPv6 组播源都创建（S，G）表项，这将占用大量的系统资源。为了解决这个问题，提出了 IPv6 双向 PIM 的概念。IPv6 双向 PIM 由 IPv6 PIM-SM 发展而来，它通过建立以 RP 为中心、分别连接 IPv6 组播源和接收者的双向 RPT，使 IPv6 组播数据沿着双向 RPT 从 IPv6 组播源经由 RP 转发到接收者。这样，在每台路由器上只需维护（*，G）表项即可，从而节约了系统资源。

IPv6 双向 PIM 主要适用于 IPv6 组播源和接收者都比较密集的网络，其工作机制如下：

1. 邻居发现

IPv6 双向PIM使用与IPv6 PIM-SM完全相同的邻居发现机制，具体请参见“1.1.2 1. 邻居发现”一节。

2. RP发现

IPv6 双向PIM使用与IPv6 PIM-SM完全相同的RP发现机制，具体请参见“1.1.2 3. RP发现”一节。

IPv6 PIM-SM 的 RP 必须指定为一个实际存在的 IPv6 地址，而 IPv6 双向 PIM 的 RP 则可以指定为一个实际不存在的 IPv6 地址，简称 RPA（Rendezvous Point Address，汇集点地址）。RPA 所属网段对应的链路就称为 RPL（Rendezvous Point Link，汇集点链路），连接到 RPL 上的所有接口都可以充当 RP，且互为备份。

说明

IPv6 双向 PIM 中的 RPF 接口是指向 RP 的接口，RPF 邻居自然是到达 RP 的下一跳地址。

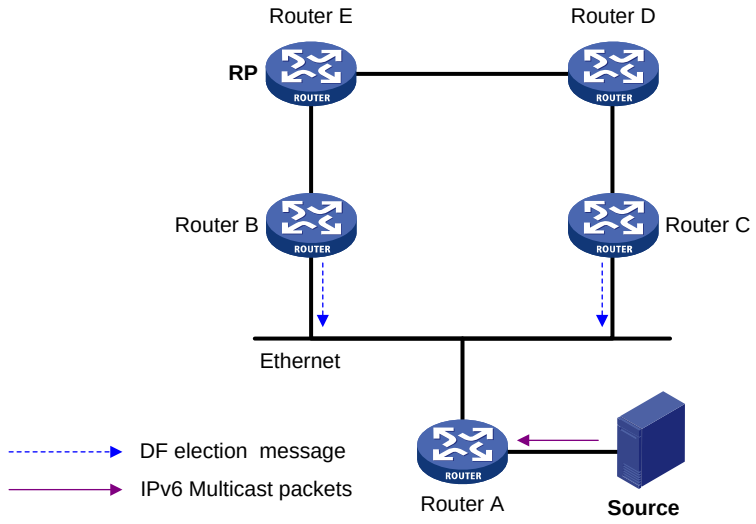
3. DF选举

DF（Designated Forwarder，指定转发者）是 IPv6 双向 PIM 中的重要角色，IPv6 组播数据由 IPv6 组播源向 RP 转发的动力来自于 DF，也就是说只有 DF 才有能力将 IPv6 组播数据向 RP 方向转发。因此，每个 RP 在每个网段都需要有其对应的 DF，以负责将该网段的 IPv6 组播数据向该 RP 转发；此外，在有多台 IPv6 组播路由器的网段，DF 的唯一性也可以避免相同的 IPv6 组播报文被重复发往 RP。

说明

在 RPL 上不需要选举 DF。

图1-8 DF 选举示意图



如 图 1-8 所示，Router B和Router C都可以从Router A收到由IPv6 组播源向IPv6 组播组G发送的IPv6 组播报文，如果它们都向下游节点转发该报文，RP最终将收到两份相同的IPv6 组播报文。因此，Router B和Router C一旦获得RP的信息，就会为该RP发起DF的选举：Router B和Router C将分别向本网段的所有IPv6 PIM路由器以组播方式发送DF选举报文（DF Election Message），该报文携带有以下信息：RP的地址、到RP的IPv6 单播路由/IPv6 MBGP路由/IPv6 组播静态路由的优先级和度量值。通过一定规则对这些参数进行比较后，Router B和Router C中的获胜者将成为DF，具体的比较规则如下：

(1) 到 RP 的优先级较高者获胜；

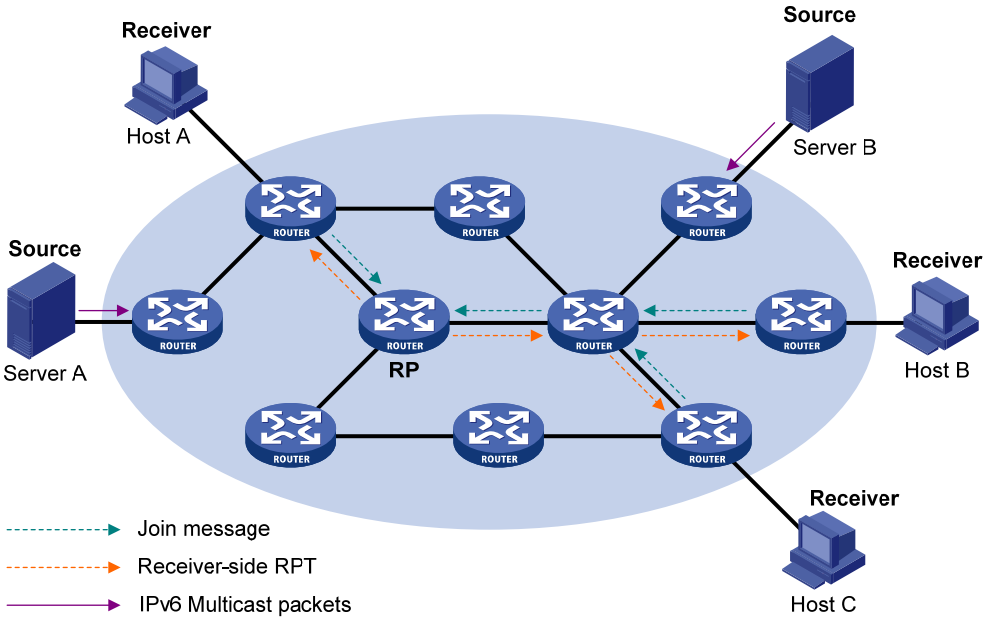
(2) 如果到 RP 的优先级相等，那么到 RP 的度量值较小者获胜；

(3) 如果到 RP 的度量值也相等，则接口的 IPv6 链路本地地址较大者获胜。

4. 构建双向RPT

双向 RPT 由两部分构成：一部分是以 RP 为根、以直连接收者的路由器为叶子的 RPT，简称接收者侧 RPT；而另一部分则是以 RP 为根、以直连 IPv6 组播源的路由器为叶子的 RPT，简称组播源侧 RPT。这两部分 RPT 的构建过程不同，下面分别加以介绍。

图1-9 接收者侧 RPT 构建示意图



接收者侧RPT的构建过程与IPv6 PIM-SM中RPT的构建过程类似，如 图 1-9 所示，其构建过程如下：

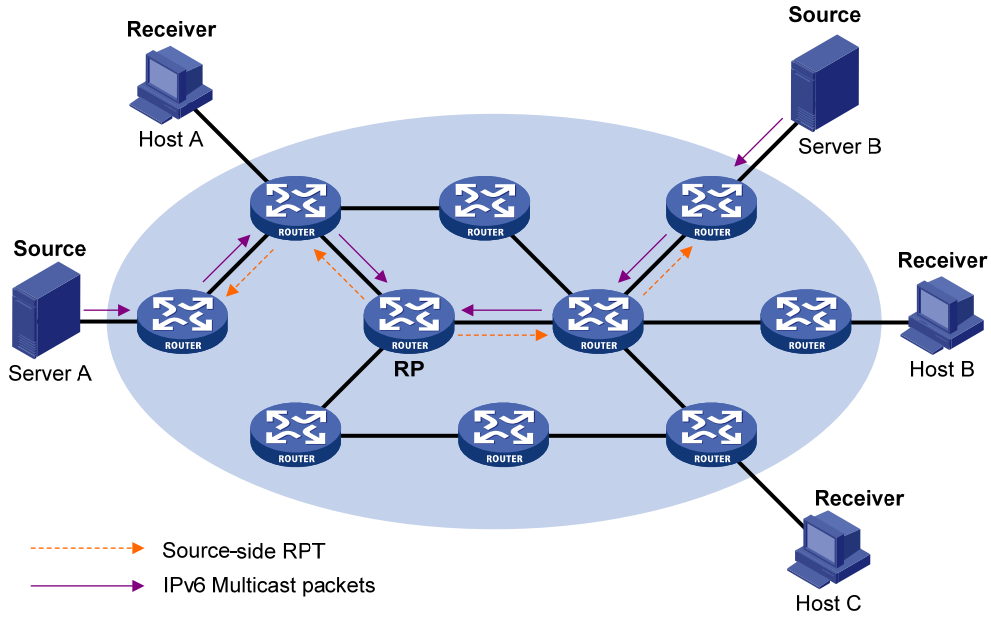
(1) 当接收者加入一个 IPv6 组播组 G 时，先通过 MLD 报文通知与其直连的路由器；

(2) 该路由器掌握了 IPv6 组播组 G 的接收者的信息后，向该组所对应的 RP 方向逐跳发送加入报文；

(3) 从直连接收者的路由器到 RP 所经过的路由器就形成了接收者侧 RPT 的分支，这些路由器都在其转发表中生成了（*，G）表项。

当某接收者对 IPv6 组播组 G 的信息不再感兴趣时，与其直连的路由器会逆着接收者侧 RPT 向该组的 RP 方向逐跳发送剪枝报文；上游节点收到该报文后在其出接口列表中删除与下游节点相连的接口，并检查自己是否拥有该 IPv6 组播组的接收者，如果没有则继续向其上游转发该剪枝报文。

图1-10 组播源侧 RPT 构建示意图



组播源侧RPT的构建过程则相对简单，如 图 1-10 所示，其构建过程如下：

(1) IPv6 组播源发向 IPv6 组播组 G 的 IPv6 组播数据在途径的每个网段，都被该网段的 DF 无条件地向 RP 转发；

(2) 从直连组播源的路由器到 RP 所经过的路由器就形成了 IPv6 组播源侧 RPT 的分支，这些路由器都在其转发表中生成了（*，G）表项。

当双向 RPT 构建完成之后，由 IPv6 组播源发出的 IPv6 组播数据将依次沿着 IPv6 组播源侧 RPT 和接收者侧 RPT，经由 RP 转发至接收者。

说明

当接收者和 IPv6 组播源位于 RP 同一侧时，组播源侧 RPT 与接收者侧 RPT 有可能在到达 RP 之前就已汇合。在这种情况下，由该 IPv6 组播源发往该接收者的 IPv6 组播数据将在此汇合点直接被转发给该接收者，而不必经由 RP。

1.1.4 IPv6 管理域机制简介

1. 两种域机制的划分

一般情况下，在一个 IPv6 PIM-SM/IPv6 双向 PIM 域内只能有一个 BSR，并由该 BSR 负责在整个 IPv6 PIM-SM/IPv6 双向 PIM 域内宣告 RP-Set 信息，所有 IPv6 组播组的信息都在此 BSR 管理的网络范围内进行转发，我们称之为 IPv6 非管理域机制。

考虑到管理的精细化，可以将整个 IPv6 PIM-SM/IPv6 双向 PIM 域划分为一个 IPv6 Global 域（IPv6 Global-scope Zone）和多个 IPv6 管理域（IPv6 Admin-scope Zone），一方面可以有效分担单一 BSR 的管理压力，另一方面可以使用私有组地址为特定区域提供专门的服务。相应地，我们称之为 IPv6 管理域机制。

IPv6 管理域与特定 Scope 值的 IPv6 组播组相对应，针对不同的 Scope 值划分相应的 IPv6 管理域。IPv6 管理域的边界由 ZBR（Zone Border Router，区域边界路由器）构成，每个 IPv6 管理域各维护一个 BSR，为特定 Scope 值的 IPv6 组播组服务，属于此范围的 IPv6 组播协议报文（如断言报文、BSR 自举报文等）无法通过 IPv6 管理域边界。不同 IPv6 管理域所服务的 IPv6 组播组范围可以重叠，该范围内的 IPv6 组播组只在本 IPv6 管理域内有效，相当于私有组地址。而 IPv6 Global 域则可视为一种特殊的 IPv6 管理域，其维护的 BSR 为 Scope 值为 14 的 IPv6 组播组提供服务。

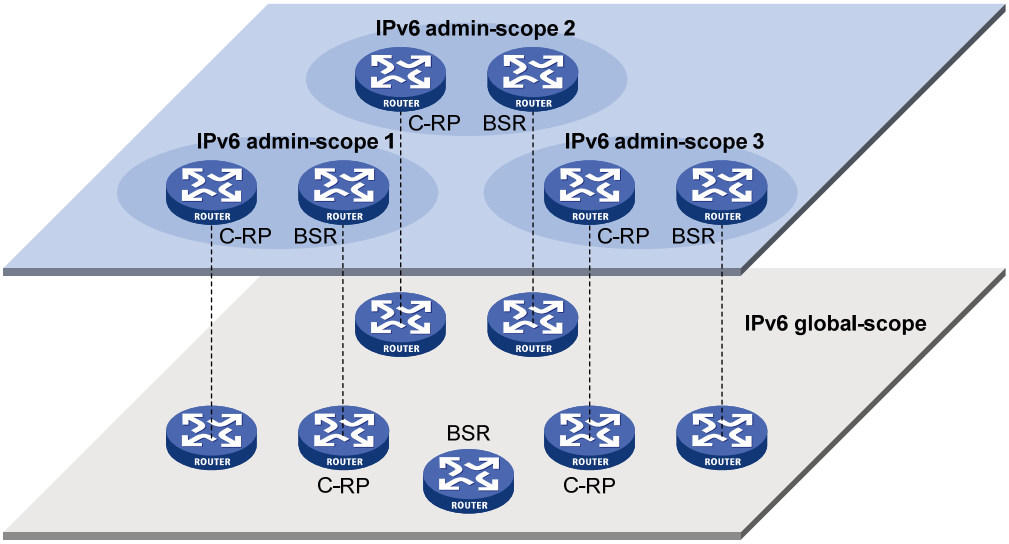
2. 管理域与Global域的关系

每个 IPv6 管理域以及 IPv6 Global 域都有独立的 C-RP 和 BSR 设备，这些设备仅在其所属的域有效，也就是说 BSR 机制与 RP 选举在各 IPv6 管理域之间是隔离的；每个 IPv6 管理域都有自己的边界，各 IPv6 管理域所服务 IPv6 组播组范围内的 IPv6 组播信息不能进、出该边界。为了更清晰地理解 IPv6 管理域和 IPv6 Global 域之间的关系，可以从以下两个角度进行考虑：

(1)　地域空间角度

IPv6 管理域是针对特定 Scope 值的逻辑管理区域，属于此范围的 IPv6 组播报文只能在本 IPv6 管理域的域内或域外传播，无法跨过 IPv6 管理域的边界。

图1-11 地域空间上 IPv6 管理域与 IPv6 Global 域的关系

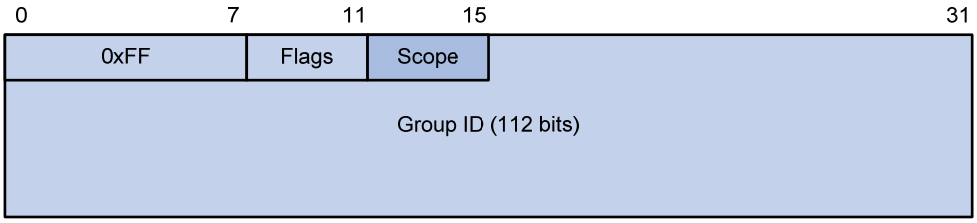


如 图 1-11 所示，对于同一Scope值的IPv6 组播组而言，各IPv6 管理域在地域上必须相互独立、相互隔离。而IPv6 Global域则包含了IPv6 PIM-SM/IPv6 双向PIM域内的所有路由器，不属于任何IPv6 管理域服务范围的IPv6 组播报文，可以在整个IPv6 PIM-SM/IPv6 双向PIM域范围内传播。

(2)　Scope 值角度

如 图 1-12 所示，IPv6 组播通过其地址结构中的Scope字段来表明该IPv6 组播组属于哪个域。

图1-12 IPv6 组播地址结构



Scope值较大的域包含Scope值较小的域，Scope值为E所对应的域（即IPv6 Global域）最大。Scope字段可能的取值及其含义如 表 1-1 所示。

表1-1 Scope 字段的取值及其含义

取值	含义	所属域
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）	IPv6管理域
4	管理本地范围（Admin-Local Scope）	IPv6管理域
5	站点本地范围（Site-Local Scope）	IPv6管理域
6、7、9～D	未分配（Unassigned）	IPv6管理域
8	机构本地范围（Organization-Local Scope）	IPv6管理域
E	全球范围（Global Scope）	IPv6 Global域

1.1.5 IPv6 PIM-SSM简介

目前，ASM（Any-Source Multicast，任意信源组播）模型包括 IPv6 PIM-DM 和 IPv6 PIM-SM 两种模式，SSM（Source-Specific Multicast，指定信源组播）模型能够借助 IPv6 PIM-SM 的部分技术来实现，也称为 IPv6 PIM-SSM。

SSM 模型为指定源组播提供了解决方案，通过 MLDv2 来维护主机与路由器之间的关系。在实际应用中，通常采用 MLDv2 以及 IPv6 PIM-SM 的一部分技术来实现 SSM 模型。由于接收者预先已知道 IPv6 组播源的具体位置，因此在 SSM 模型中无需 RP，无需构建 RPT，也无需 IPv6 组播源注册过程来发现其它 IPv6 PIM 域内的 IPv6 组播源。

IPv6 PIM-SSM 的工作机制如下：

1. 邻居发现

IPv6 PIM-SSM使用与IPv6 PIM-SM完全相同的邻居发现机制，具体请参见“1. 邻居发现”一节。

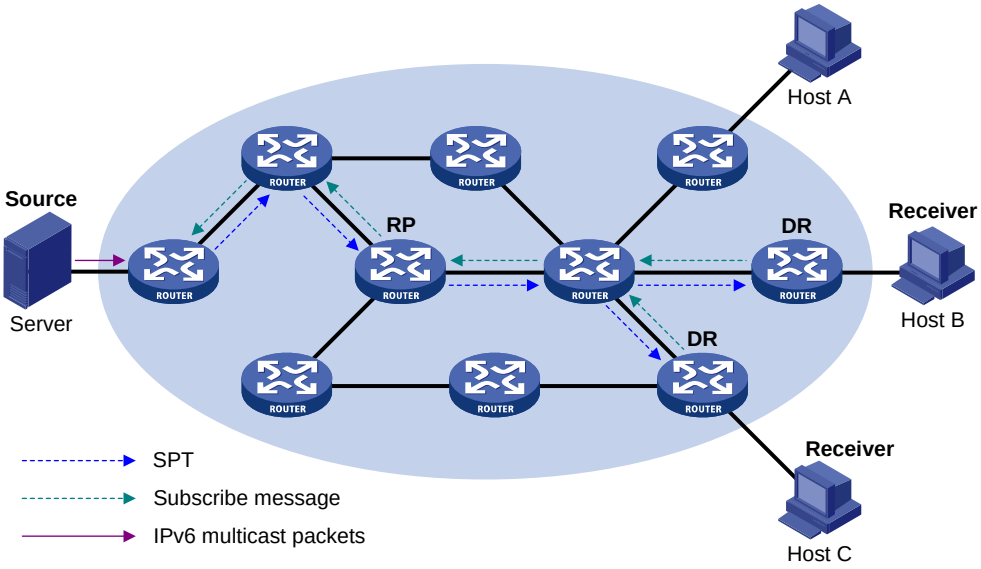
2. DR选举

IPv6 PIM-SSM使用与IPv6 PIM-SM完全相同的DR选举机制，具体请参见 “1.1.2 2. DR选举”一节。

3. 构建SPT

构建为 IPv6 PIM-SM 服务的 RPT，还是构建为 IPv6 PIM-SSM 服务的 SPT，关键在于接收者准备加入的IPv6组播组是否属于IPv6 SSM组地址范围（IANA保留的IPv6 SSM组地址范围为FF3x::/32，其中 x 表示任意合法的 scope）。

图1-13 IPv6 PIM-SSM 中构建 SPT 示意图



如 图 1-13 所示，Host B和Host C为IPv6 组播信息的接收者（Receiver），由其借助MLDv2 的报告报文向DR报告自己对来自IPv6 组播源S、发往IPv6 组播组G的信息感兴趣。收到该报告报文的DR先判断该报文中的IPv6 组地址是否在IPv6 SSM组地址范围内：

- 如果在 IPv6 SSM 组地址范围内，则构建 IPv6 PIM-SSM，并向 IPv6 组播源 S 逐跳发送通道（Channel）的订阅报文（Subscribe Message）。沿途所有路由器上都创建（S，G）表项，从而在网络内构建了一棵以 IPv6 组播源 S 为根、以接收者为叶子的 SPT，该 SPT 就是 IPv6 PIM-SSM 中的传输通道；
- 如果不在 IPv6 SSM 组地址范围内，则仍旧按照 IPv6 PIM-SM 的流程进行后续处理，此时接收者侧 DR 需要向 RP 发送（*，G）加入报文，同时 IPv6 组播源侧 DR 需要进行 IPv6 组播源的注册。

说明

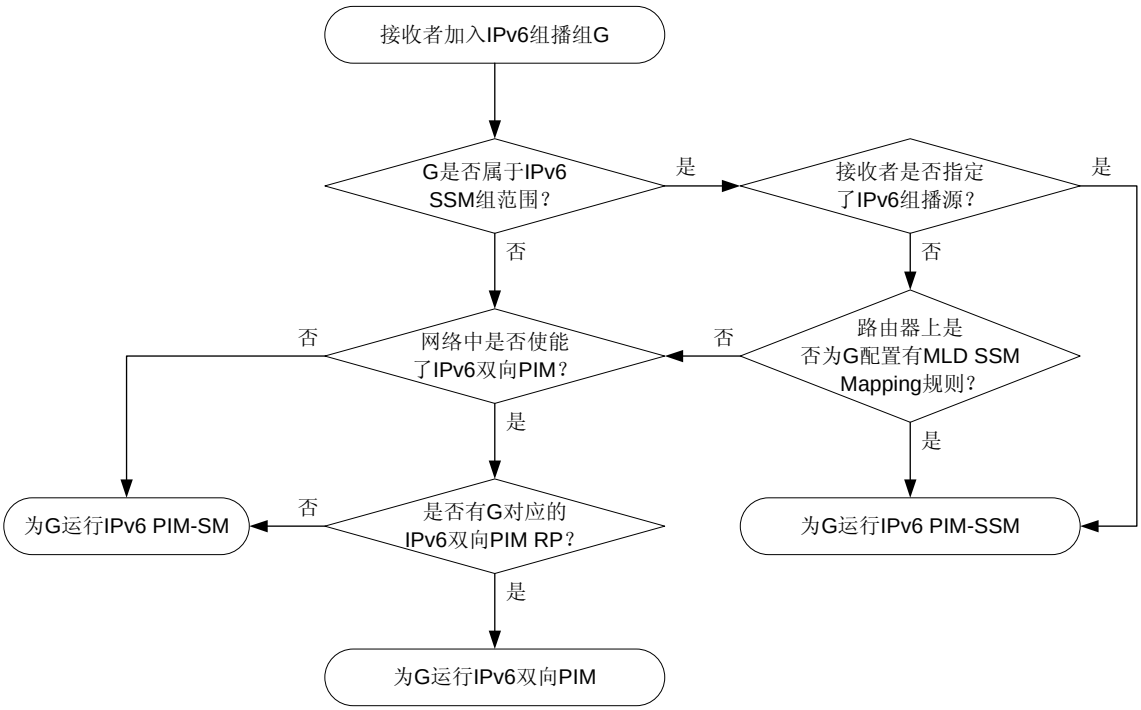
在 IPv6 PIM-SSM 中，借助“通道”的概念表示 IPv6 组播组，借助“订阅报文”的概念表示加入报文。

1.1.6 各IPv6 PIM协议运行关系

在一个 IPv6 PIM 网络中，不允许 IPv6 PIM-DM 与其它类型的 IPv6 PIM 协议（IPv6 PIM-SM、IPv6 双向 PIM 和 IPv6 PIM-SSM）同时运行，但允许同时运行 IPv6 PIM-SM、IPv6 双向 PIM 和 IPv6 PIM-SSM。

当网络中同时运行IPv6 PIM-SM、IPv6 双向PIM和IPv6 PIM-SSM时，针对具体的组加入行为运行哪种类型的IPv6 PIM协议，其判断过程如 图 1-14 所示。

图1-14 各 IPv6 PIM 协议运行关系示意图



有关 MLD SSM Mapping 的详细介绍，请参见“IP 组播配置指导”中的“MLD”。

1.1.7 多实例的IPv6 PIM

在多实例应用中，IPv6 组播路由器需要针对不同的实例分别维护 IPv6 PIM 邻居表、IPv6 组播路由表、BSR 信息和 RP-Set 信息，并保持各实例间上述信息的相互独立。

当 IPv6 组播路由器收到 IPv6 组播数据报文时，需要区分出该数据报文所属的实例，并根据该实例对应的 IPv6 组播路由表将其转发，或创建与该实例的 IPv6 PIM 相关的 IPv6 组播路由表项。

1.1.8 协议规范

与 IPv6 PIM 相关的协议规范有：

- RFC 3973：Protocol Independent Multicast-Dense Mode (PIM-DM): Protocol Specification (Revised)
- RFC 4601：Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised)
- RFC 4610：Anycast-RP Using Protocol Independent Multicast (PIM)
- RFC 3956：Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address
- RFC 5015：Bidirectional Protocol Independent Multicast (BIDIR-PIM)
- RFC 5059：Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
- RFC 4607：Source-Specific Multicast for IP

- draft-ietf-ssm-overview-05：An Overview of Source-Specific Multicast (SSM)

1.2 配置IPv6 PIM-DM

1.2.1 IPv6 PIM-DM配置任务简介

表1-2 IPv6 PIM-DM 配置任务简介

配置任务	说明	详细配置
使能IPv6 PIM-DM	必选	1.2.3
使能状态刷新能力	可选	1.2.4
配置状态刷新参数	可选	1.2.5
配置IPv6 PIM-DM定时器	可选	1.2.6
配置IPv6 PIM公共特性	可选	1.6

1.2.2 配置准备

在配置 IPv6 PIM-DM 之前，需完成以下任务：

- 配置任一 IPv6 单播路由协议，实现域内网络层互通

1.2.3 使能IPv6 PIM-DM

提示

同一台设备相同实例的所有接口上启用的 IPv6 PIM 模式必须相同。

在进行各项 IPv6 PIM 配置之前，必须先使能 IPv6 组播路由。

在接口上使能了 IPv6 PIM-DM 后，路由器之间才能够建立 IPv6 PIM 邻居，从而对来自 IPv6 PIM 邻居的协议报文进行处理。在部署 IPv6 PIM-DM 域时，建议在其所有非边界接口上均使能 IPv6 PIM-DM。

表1-3 使能 IPv6 PIM-DM

操作	命令	说明
进入系统视图	**system-view**	-
使能IPv6组播路由，并进入IPv6 MRIB视图	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	缺省情况下，IPv6组播路由处于关闭状态 本命令的详细介绍请参见“IP组播命令参考”中的“IPv6组播路由与转发”
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能IPv6 PIM-DM	**ipv6 pim dm**	缺省情况下，IPv6 PIM-DM处于关闭状态

1.2.4 使能状态刷新能力

为了避免各路由器上被剪枝的接口因为超时而恢复转发，与 IPv6 组播源直连的路由器会周期性地发送（S，G）状态刷新报文，该报文沿着 IPv6 PIM-DM 域最初的扩散路径逐跳进行转发，从而刷新沿途所有路由器上的剪枝定时器的状态。只有当一个共享网段内的所有 IPv6 PIM 路由器上都使能了状态刷新能力时，该共享网段才具备状态刷新能力。

请在 IPv6 PIM-DM 域内的所有路由器上进行如下配置。

表1-4 使能状态刷新能力

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能状态刷新能力	**ipv6 pim state-refresh-capable**	缺省情况下，状态刷新能力处于使能状态

1.2.5 配置状态刷新参数

直连 IPv6 组播源的路由器会以一定的时间间隔周期性地发送状态刷新报文，可以在与 IPv6 组播源直连的路由器上通过配置来改变这个时间间隔。

路由器可能在短时间内收到多个状态刷新报文，而其中有些报文可能是重复的。为了避免接收这些重复的报文，可以配置接收新状态刷新报文的等待时间：路由器将丢弃在该时间内收到的状态刷新报文；当该时间超时后，路由器将正常接收新的状态刷新报文，并更新自己的 IPv6 PIM-DM 状态，同时重置该等待时间。

在收到状态刷新报文时，路由器会将该报文的 Hop Limit 值减 1 后转发给其下游，直至该报文的 Hop Limit 值减为 0，当网络规模很小时，状态刷新报文将在网络中循环传递。因此，为了有效控制刷新报文的传递范围，需要根据网络规模大小在与 IPv6 组播源直连的路由器上配置合适的 Hop Limit 值。

表1-5 配置状态刷新参数

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
配置发送状态刷新报文的时间间隔	**state-refresh-interval** *interval*	缺省情况下，发送状态刷新报文的时间间隔为60秒
配置接收新状态刷新报文的等待时间	**state-refresh-rate-limit** *time*	缺省情况下，接收新状态刷新报文的等待时间为30秒
配置状态刷新报文的Hop Limit值	**state-refresh-hoplimit** *hoplimit-value*	缺省情况下，状态刷新报文的Hop Limit值为255

1.2.6 配置IPv6 PIM-DM定时器

嫁接报文是 IPv6 PIM-DM 中唯一使用确认机制的报文。在 IPv6 PIM-DM 域中，下游路由器发出嫁接报文后，如果在指定时间内没有收到来自其上游路由器的嫁接应答报文，则会重发嫁接报文，直到被确认。

有关IPv6 PIM-DM其它定时器的相关配置，请参见“1.6.6 配置IPv6 PIM公共定时器”。

表1-6 配置 IPv6 PIM-DM 定时器

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置嫁接报文的重传时间	**ipv6 pim timer graft-retry** *interval*	缺省情况下，嫁接报文的重传时间为3秒

1.3 配置IPv6 PIM-SM

1.3.1 IPv6 PIM-SM配置任务简介

表1-7 IPv6 PIM-SM 配置任务简介

配置任务		说明	详细配置
使能IPv6 PIM-SM		必选	1.3.3
配置RP	配置静态RP	二者至少选其一，若只配置静态RP，则不必再配置BSR	1.3.4 1.
	配置C-RP		1.3.4 2.
	配置Anycast-RP	可选	1.3.4 3.
配置BSR	配置C-BSR	必选	1.3.5 1.
	配置BSR服务边界	可选	1.3.5 2.
	关闭自举报文语义分片功能	可选	1.3.5 3.
配置IPv6组播源注册		可选	1.3.6
配置SPT切换		可选	1.3.7
配置IPv6 PIM公共特性		可选	1.6

1.3.2 配置准备

在配置 IPv6 PIM-SM 之前，需完成以下任务：

- 配置任一 IPv6 单播路由协议，实现域内网络层互通

1.3.3 使能IPv6 PIM-SM

提示

同一台设备相同实例的所有接口上启用的 IPv6 PIM 模式必须相同。

在进行各项 IPv6 PIM 配置之前，必须先使能 IPv6 组播路由。

在接口上使能了 IPv6 PIM-SM 后，路由器之间才能够建立 IPv6 PIM 邻居，从而对来自 IPv6 PIM 邻居的协议报文进行处理。在部署 IPv6 PIM-SM 域时，建议在其所有非边界接口上均使能 IPv6 PIM-SM。

表1-8 使能 IPv6 PIM-SM

操作	命令	说明
进入系统视图	**system-view**	-
使能IPv6组播路由，并进入IPv6 MRIB视图	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	缺省情况下，IPv6组播路由处于关闭状态 本命令的详细介绍请参见“IP组播命令参考”中的“IPv6组播路由与转发”
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能IPv6 PIM-SM	**ipv6 pim sm**	缺省情况下，IPv6 PIM-SM处于关闭状态

1.3.4 配置RP

一个 RP 可以为多个 IPv6 组播组服务，也可以为所有 IPv6 组播组服务。每个 IPv6 组播组在任意时刻，只能由唯一的一个 RP 为其转发数据，而不能由多个 RP 转发数据。

RP 可以通过手工方式静态配置，也可以通过 BSR 机制动态选举。由于在大型 IPv6 PIM 网络中配置静态 RP 将非常繁琐，因此，通常将静态 RP 作为动态选举 RP 机制的备份手段，以提高网络的健壮性，增强组播网络的运营管理能力。

1. 配置静态RP

当网络内仅有一个动态 RP 时，可以手工配置静态 RP，既可避免因单一节点故障而引起的通信中断，也可避免 C-RP 与 BSR 之间频繁的信息交互而占用带宽。IPv6 PIM-SM 域内的所有路由器上都必须进行完全相同的静态 RP 配置。

表1-9 配置静态 RP

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
配置服务于IPv6 PIM-SM的静态RP	**static-rp** *ipv6-rp-address* [*acl6-number* | **preferred**] *	必选 缺省情况下，没有配置静态RP

2. 配置C-RP

提示

在配置 C-RP 时，应在 C-RP 与 IPv6 PIM-SM 域中的其它设备之间保留较大的通信带宽。

在 IPv6 PIM-SM 域中，可以把有意成为 RP 的路由器配置为 C-RP。BSR 通过接收来自 C-RP 的 C-RP 信息，或者接收来自其它路由器的自动 RP 宣告，收集 C-RP 信息并将其汇总为 RP-Set 信息，然后在全网内扩散。之后，网络内的其它路由器根据 RP-Set 信息计算出特定组播组范围所对应的 RP。建议在骨干网路由器上配置 C-RP。

为了使 BSR 能够在 IPv6 PIM-SM 域内分发 RP-Set 信息，C-RP 必须周期性地向 BSR 发送宣告报文，BSR 从该报文中学习 RP-Set 信息，并将该信息与自己的 IPv6 地址一起封装在自举报文中向域中的所有 IPv6 PIM 路由器进行宣告。

C-RP 在其宣告报文中封装一个保持时间，BSR 在收到该报文后，从中获得该时间值并启动 C-RP 超时定时器，如果超时后 BSR 仍没有收到来自 C-RP 后续的宣告报文，则认为目前网络中的 C-RP 失效或不可达。

为了防止 C-RP 欺骗，需要在 BSR 上配置合法的 C-RP 地址范围及其服务的组播组范围。同时由于每个 C-BSR 都可能成为 BSR，因此必须在 IPv6 PIM-SM 域内的所有 C-BSR 上都配置相同的过滤策略。

表1-10 配置 C-RP

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
配置C-RP	**c-rp** *ipv6-address* [**advertisement-interval** *adv-interval* | { **group-policy** *acl6-number* | **scope** *scope-id* } | **holdtime** *hold-time* | **priority** *priority*] *	缺省情况下，没有配置C-RP
（可选）配置合法的C-RP地址范围及其服务的IPv6组播组范围	**crp-policy** *acl6-number*	缺省情况下，C-RP地址范围及其服务的IPv6组播组范围不受任何限制

3. 配置Anycast-RP

在配置 Anycast-RP 前，需要先在 IPv6 PIM-SM 域中完成静态 RP 或 C-RP 的配置，然后将静态 RP 或动态选举出的 RP 当作 Anycast-RP 地址进行 Anycast-RP 的配置。

在配置 Anycast-RP 时，请遵循以下原则：

- Anycast-RP 集中必须包括 Anycast-RP 地址所在的设备。
- 在 Anycast-RP 集的每台成员设备上通过重复执行 **anycast-rp** 命令，将包括自己在内的所有成员的地址都添加到 Anycast-RP 集中。

提示

- Anycast-RP 地址不能再用作 BSR 的地址，否则其发出的自举报文将被其它成员设备丢弃。
- 一个 Anycast-RP 集中的成员设备不建议超过 16 台，否则将影响网络性能。
- 建议使用 LoopBack 接口的地址作为 Anycast-RP 成员地址。如果一台成员设备有多个接口的地址被添加到 Anycast-RP 集中，则采用 IPv6 地址最小的那个作为其成员地址，其余作为备份。

表1-11 配置 Anycast-RP

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
配置Anycast-RP	**anycast-rp** *ipv6-anycast-rp-address ipv6-member-address*	缺省情况下，没有配置Anycast-RP

1.3.5 配置BSR

如果配置了静态 RP，则不需要配置 BSR；但如果配置了 C-RP 来动态选举 RP，则必须配置 BSR。在一个 IPv6 PIM-SM 域中只能有一个 BSR，但需要配置至少一个 C-BSR。任意一台路由器都可以被配置为 C-BSR。在 C-BSR 之间通过自动选举产生 BSR，BSR 负责在 IPv6 PIM-SM 域中收集并发布 RP 信息。

1. 配置C-BSR

提示

由于 BSR 与 IPv6 PIM-SM 域中的其它设备需要交换大量信息，因此应在 C-BSR 与 IPv6 PIM-SM 域中的其它设备之间保留较大的通信带宽。

C-BSR 应配置在骨干网的路由器上，C-BSR 间的自动选举机制简单描述如下：

- 最初，每个 C-BSR 都认为自己是本 IPv6 PIM-SM 域的 BSR，向其它路由器发送自举报文；
- 当某 C-BSR 收到其它 C-BSR 发来的自举报文时，首先比较自己与后者的优先级，优先级较高者获胜；在优先级相同的情况下，再比较自己与后者的 BSR 地址，拥有较大 IPv6 地址者获胜。如果后者获胜，则用后者的 BSR 地址替换自己的 BSR 地址，并不再认为自己是 BSR；否则，保留自己的 BSR 地址，并继续认为自己是 BSR。

在一个 IPv6 PIM-SM 域中，从众多 C-BSR 中选举出唯一的 BSR。IPv6 PIM-SM 域内的 C-RP 向 BSR 发送宣告报文，由 BSR 汇总为 RP-Set，并向本 IPv6 PIM-SM 域内的所有路由器进行宣告。所有路由器都使用统一的哈希算法，得到特定 IPv6 组播组所对应 RP 的地址。

通过在路由器上配置合法 BSR 的地址范围，可以对收到的自举报文按照地址范围进行过滤，从而防止某些恶意主机非法伪装成 BSR，以避免合法的 BSR 被恶意取代。必须在 IPv6 PIM-SM 域内的所有路由器上进行相同的配置。通常针对以下两类情况实施预防措施：

- 某些恶意主机通过伪造自举报文以欺骗路由器，试图更改 RP 映射关系。这种攻击通常发生在边缘路由器上，由于 BSR 处于网络内部，主机在网络外部，因此边缘路由器通过对收到的自举报文进行邻居检查和 RPF 检查，丢弃不符合要求的报文，就可以避免外部网络用户对内部网络 BSR 的攻击；
- 网络中某台路由器被攻击者控制，或者有非法接入的路由器时，攻击者可以将这样的路由器配置为 C-BSR，并使其在竞争中获胜，从而控制网络中 RP 信息的发布权。由于在被配置为 C-BSR 后，路由器会自动向整个网络扩散自举报文，而自举报文是 Hop Limit 值为 1 的 IPv6 组播报文，所以只要其邻居路由器不接收该自举报文，就不会影响整个网络。因此，通过在整个网络的所有路由器上都配置合法 BSR 的地址范围，从而丢弃合法范围之外的自举报文，就可以防止此类攻击。

以上两种预防措施可以部分地保护网络中 BSR 的安全。但是如果某台合法的 BSR 路由器被攻击者控制，还是可能导致问题。

表1-12 配置 C-BSR

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
配置C-BSR	**c-bsr** *ipv6-address* [**scope** *scope-id*] [**hash-length** *hash-length* | **priority** *priority*] *	缺省情况下，没有配置C-BSR
（可选）配置合法的BSR地址范围	**bsr-policy** *acl6-number*	缺省情况下，BSR的地址范围不受任何限制

2. 配置BSR服务边界

BSR 作为 IPv6 PIM-SM 域中的管理核心，负责将收集到的 RP-Set 信息以自举报文的形式发向 IPv6 PIM-SM 域中的所有路由器。

BSR 的服务边界，即 IPv6 PIM-SM 域的边界。BSR 是针对特定的服务范围而言的，众多的 BSR 服务边界接口将网络划分成不同的 IPv6 PIM-SM 域，自举报文无法通过 IPv6 PIM-SM 域的边界，BSR 服务边界之外的路由器也不能参与本 IPv6 PIM-SM 域内的组播转发。

请在欲配置为 BSR 服务边界的路由器上进行如下配置。

表1-13 配置 BSR 服务边界

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置BSR的服务边界	**ipv6 pim bsr-boundary**	缺省情况下，没有配置BSR的服务边界

3. 关闭自举报文语义分片功能

BSR 周期性地向所在 IPv6 PIM-SM 域发送自举报文以通告 RP-Set 信息。当 RP-Set 信息较少时，自举报文被封装在一个 IPv6 报文中发送出去；而当 RP-Set 信息较多时，自举报文的大小可能超过

接口的 MTU（Maximum Transmission Unit，最大传输单元）值，从而触发其在 IP 层的分片。在这种情况下，一个 IP 分片的丢失就会导致整个自举报文都被丢弃。

自举报文语义分片功能可以解决上述问题：当自举报文大于接口 MTU 时，会被分解为多个自举报文分片（Bootstrap Message Fragment，BSMF）。非 BSR 收到自举报文分片后，若发现某组范围对应的 RP 信息都在这一个分片中，便立即更新该组范围对应的 RP-Set；若发现某组范围映射的 RP 信息被分在了多个分片中，则待收齐了这些分片后再更新该组范围对应的 RP-Set。这样，由于不同分片所含组范围对应的 RP 信息不同，因此个别分片的丢失只影响该分片所含组范围对应的 RP 信息，而不会导致整个自举报文都被丢弃。

自举报文语义分片功能是缺省使能的，但由于不支持该功能的设备会将自举报文分片当作完整的自举报文处理，从而导致其学到的 RP-Set 信息不完整，因此当 IPv6 PIM-SM 域中存在此类设备时，请在已配置为 C-BSR 的路由器上关闭本功能。

表1-14 关闭自举报文语义分片功能

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
关闭自举报文语义分片功能	**undo bsm-fragment enable**	缺省情况下，自举报文语义分片功能处于使能状态

说明

通常，BSR 根据其 BSR 接口的 MTU 值对自举报文进行语义分片；而对由于新学到 IPv6 PIM 邻居而触发的自举报文发送，则根据发送接口的 MTU 值进行语义分片。

1.3.6 配置IPv6 组播源注册

在 IPv6 PIM-SM 域内，IPv6 组播源侧 DR 向 RP 发送注册报文，而这些注册报文拥有不同的 IPv6 组播源或 IPv6 组播地址。为了让 RP 服务于特定的 IPv6 组播组，可以对注册报文进行过滤。如果某个（S，G）表项被过滤规则拒绝，或者过滤规则中没有定义对它的操作，RP 都会向 DR 发送注册停止报文，以停止该 IPv6 组播数据的注册过程。

考虑到注册报文在传递过程中的完整性，可以配置根据整个报文来计算校验和。但为了减少往注册报文中封装数据报文的工作量并考虑到互通性，一般情况下不建议配置根据注册报文的全部内容来计算校验和的方式。

当接收者不再通过 RP 接收发往某 IPv6 组播组的数据（即 RP 不再服务于该 IPv6 组播组），或 RP 开始接收 IPv6 组播源沿着 SPT 发来的 IPv6 组播数据时，RP 将向 IPv6 组播源侧 DR 发送注册停止报文，DR 收到该报文后将停止发送封装有 IPv6 组播数据的注册报文并启动注册停止定时器（Register-Stop Timer）。在注册停止定时器超时之前，DR 会向 RP 发送一个空注册报文（Null-Register Message，即不封装 IPv6 组播数据的注册报文）：如果 DR 在注册探测时间（Register_Probe_Time）内收到了来自 RP 的注册停止报文，DR 将刷新其注册停止定时器；否则，DR 将重新开始发送封装有 IPv6 组播数据的注册报文。

注册停止定时器的超时时间是一个随机值，由其它两个时间值决定：注册抑制时间（Register_Suppression_Time）和注册探测时间（固定为 5 秒）。其具体取值范围如下：（0.5×注册抑制时间，1.5×注册抑制时间）－注册探测时间。

请在所有已配置为 C-RP 的路由器上配置注册报文的过滤规则和根据注册报文的全部内容来计算校验和；请在所有可能成为 IPv6 组播源侧 DR 的路由器上配置注册抑制时间。

表1-15 配置 IPv6 组播源注册

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
配置注册报文的过滤规则	**register-policy** *acl6-number*	缺省情况下，没有配置注册报文的过滤规则
配置根据注册报文的全部内容来计算校验和	**register-whole-checksum**	缺省情况下，仅根据注册报文头来计算校验和
配置注册抑制时间	**register-suppression-timeout** *interval*	缺省情况下，注册抑制时间为60秒

1.3.7 配置SPT切换

接收者侧 DR 和 RP 都能够周期性地检测流经本设备的 IPv6 组播数据的转发速率（交换机无此功能），从而触发从 RPT 切换到 SPT。

提示

由于某些设备无法将 IPv6 组播报文封装在注册报文中发给 RP，因此在可能成为 RP 的设备上不建议配置永不发起 SPT 切换，以免导致 IPv6 组播报文转发失败。

表1-16 配置 SPT 切换

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
配置发起SPT切换的条件	**spt-switch-threshold** { *traffic-rate* | **immediacy** | **infinity** } [**group-policy** *acl6-number*]	缺省情况下，设备收到第一个IPv6组播数据包后便立即向SPT切换 交换机不支持*traffic-rate*参数

1.4 配置IPv6双向PIM

1.4.1 IPv6 双向PIM配置任务简介

表1-17 IPv6 双向 PIM 配置任务简介

配置任务		说明	详细配置
使能IPv6双向PIM		必选	1.4.3
配置RP	配置静态RP	二者至少选其一，若只配置静态RP，则不必再配置BSR	1.4.4 1.
	配置C-RP		1.4.4 2.
	配置IPv6双向PIM RP的最大数目	可选	1.4.4 3.
配置BSR	配置C-BSR	必选	1.4.5 1.
	配置BSR服务边界	可选	1.4.5 2.
	关闭自举报文语义分片功能	可选	1.4.5 3.
配置IPv6 PIM公共特性		可选	1.6

1.4.2 配置准备

在配置 IPv6 双向 PIM 之前，需完成以下任务：

- 配置任一 IPv6 单播路由协议，实现域内网络层互通

1.4.3 使能IPv6 双向PIM

提示

同一台设备相同实例的所有接口上启用的 IPv6 PIM 模式必须相同。

由于 IPv6 双向 PIM 是在 IPv6 PIM-SM 的基础上实现的，因此在使能 IPv6 双向 PIM 之前须先使能 IPv6 PIM-SM。在部署 IPv6 双向 PIM 域时，建议在其所有非边界接口上均使能 IPv6 PIM-SM。

表1-18 使能 IPv6 双向 PIM

操作	命令	说明
进入系统视图	**system-view**	-
使能IPv6组播路由，并进入MRIB视图	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	缺省情况下，IPv6组播路由处于关闭状态 本命令的详细介绍请参见“IP组播命令参考”中的“IPv6组播路由与转发”
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能IPv6 PIM-SM	**ipv6 pim sm**	缺省情况下，IPv6 PIM-SM处于关闭状态

操作	命令	说明
退回系统视图	**quit**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
使能IPv6双向PIM	**bidir-pim enable**	缺省情况下，IPv6双向PIM处于关闭状态

1.4.4 配置RP

提示

当 IPv6 PIM 网络中同时运行 IPv6 PIM-SM 和 IPv6 双向 PIM 时，请勿使一个 RP 同时为 IPv6 PIM-SM 和 IPv6 双向 PIM 工作，否则可能引起 IPv6 PIM 路由表出错。

一个 RP 可以为多个 IPv6 组播组服务，也可以为所有 IPv6 组播组服务。每个 IPv6 组播组在任意时刻，只能由唯一的一个 RP 为其转发数据，而不能由多个 RP 转发数据。

RP 可以通过手工方式静态配置，也可以通过 BSR 机制动态选举。由于在大型 IPv6 PIM 网络中配置静态 RP 将非常繁琐，因此，通常将静态 RP 作为动态选举 RP 机制的备份手段，以提高网络的健壮性，增强组播网络的运营管理能力。

1. 配置静态RP

当网络内仅有一个动态 RP 时，可以手工配置静态 RP，既可避免因单一节点故障而引起的通信中断，也可避免 C-RP 与 BSR 之间频繁的信息交互而占用带宽。IPv6 双向 PIM 域内的所有路由器上都必须进行完全相同的静态 RP 配置。

说明

IPv6 双向 PIM 允许将静态 RP 的 IPv6 地址指定为一个实际不存在的 IPv6 地址。譬如，一条链路两端接口的 IPv6 地址分别为 1001::1/64 和 1001::2/64，可以将静态 RP 的 IPv6 地址指定为同网段但实际不存在的一个地址，如 1001::100/64，该链路就成为了 RPL。

表1-19 配置静态 RP

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
配置服务于IPv6双向PIM的静态RP	**static-rp** *ipv6-rp-address* **bidir** [*acl6-number* | **preferred**] *	必选 缺省情况下，没有配置静态RP

2. 配置C-RP

提示

在配置 C-RP 时，应在 C-RP 与 IPv6 双向 PIM 域中的其它设备之间保留较大的通信带宽。

在 IPv6 双向 PIM 域中，可以把有意成为 RP 的路由器配置为 C-RP。BSR 通过接收来自 C-RP 的 C-RP 信息，或者接收来自其它路由器的自动 RP 宣告，收集 C-RP 信息并将其汇总为 RP-Set 信息，然后在全网内扩散。之后，网络内的其它路由器根据 RP-Set 信息计算出特定组播组范围所对应的 RP。建议在骨干网路由器上配置 C-RP。

为了使 BSR 能够在 IPv6 双向 PIM 域内分发 RP-Set 信息，C-RP 必须周期性地向 BSR 发送宣告报文，BSR 从该报文中学习 RP-Set 信息，并将该信息与自己的 IPv6 地址一起封装在自举报文中向域中的所有 IPv6 PIM 路由器进行宣告。

C-RP 在其宣告报文中封装一个保持时间，BSR 在收到该报文后，从中获得该时间值并启动 C-RP 超时定时器，如果超时后 BSR 仍没有收到来自 C-RP 后续的宣告报文，则认为目前网络中的 C-RP 失效或不可达。

表1-20 配置 C-RP

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
配置服务于IPv6双向PIM的C-RP	**c-rp** *ipv6-address* [**advertisement-interval** *adv-interval* | { **group-policy** *acl6-number* | **scope** *scope-id* } | **holdtime** *hold-time* | **priority** *priority*] * **bidir**	缺省情况下，没有配置C-RP

3. 配置IPv6 双向PIM RP的最大数目

由于 IPv6 双向 PIM 为每个 RP 都要在所有 IPv6 PIM 接口上进行 DF 选举，因此实际组网中不建议配置多个 IPv6 双向 PIM RP。通过本配置可以限制 IPv6 双向 PIM RP 的数目，超出限制值的 RP 不会生效，仅能进行 DF 选举而无法指导转发。

提示

在配置 IPv6 双向 PIM RP 的最大数目时，如果现有 IPv6 双向 PIM RP 的数目已超过配置值，系统不会自动删除超出限制值的 RP，用户可根据需要进行手工删除。

表1-21 配置 IPv6 双向 PIM RP 的最大数目

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
配置IPv6双向PIM RP的最大数目	**bidir-rp-limit** *limit*	缺省情况下，双向PIM RP的最大数目为6

1.4.5 配置BSR

如果配置了静态 RP，则不需要配置 BSR；但如果配置了 C-RP 来动态选举 RP，则必须配置 BSR。在一个 IPv6 双向 PIM 域中只能有一个 BSR，但需要配置至少一个 C-BSR。任意一台路由器都可以被配置为 C-BSR。在 C-BSR 之间通过自动选举产生 BSR，BSR 负责在 IPv6 双向 PIM 域中收集并发布 RP 信息。

1. 配置C-BSR

提示

由于 BSR 与 IPv6 双向 PIM 域中的其它设备需要交换大量信息，因此应在 C-BSR 与 IPv6 双向 PIM 域中的其它设备之间保留较大的通信带宽。

C-BSR 应配置在骨干网的路由器上，C-BSR 间的自动选举机制简单描述如下：

- 最初，每个 C-BSR 都认为自己是本 IPv6 双向 PIM 域的 BSR，向其它路由器发送自举报文；
- 当某 C-BSR 收到其它 C-BSR 发来的自举报文时，首先比较自己与后者的优先级，优先级较高者获胜；在优先级相同的情况下，再比较自己与后者的 BSR 地址，拥有较大 IPv6 地址者获胜。如果后者获胜，则用后者的 BSR 地址替换自己的 BSR 地址，并不再认为自己是 BSR；否则，保留自己的 BSR 地址，并继续认为自己是 BSR。

在一个 IPv6 双向 PIM 域中，从众多 C-BSR 中选举出唯一的 BSR。IPv6 双向 PIM 域内的 C-RP 向 BSR 发送宣告报文，由 BSR 汇总为 RP-Set，并向本 IPv6 双向 PIM 域内的所有路由器进行宣告。所有路由器都使用统一的哈希算法，得到特定 IPv6 组播组所对应 RP 的地址。

通过在路由器上配置合法 BSR 的地址范围，可以对收到的自举报文按照地址范围进行过滤，从而防止某些恶意主机非法伪装成 BSR，以避免合法的 BSR 被恶意取代。必须在 IPv6 双向 PIM 域内的所有路由器上进行相同的配置。通常针对以下两类情况实施预防措施：

- 某些恶意主机通过伪造自举报文以欺骗路由器，试图更改 RP 映射关系。这种攻击通常发生在边缘路由器上，由于 BSR 处于网络内部，主机在网络外部，因此边缘路由器通过对收到的自举报文进行邻居检查和 RPF 检查，丢弃不符合要求的报文，就可以避免外部网络用户对内部网络 BSR 的攻击；
- 网络中某台路由器被攻击者控制，或者有非法接入的路由器时，攻击者可以将这样的路由器配置为 C-BSR，并使其在竞争中获胜，从而控制网络中 RP 信息的发布权。由于在被配置为 C-BSR 后，路由器会自动向整个网络扩散自举报文，而自举报文是 Hop Limit 值为 1 的 IPv6 组播报文，所以只要其邻居路由器不接收该自举报文，就不会影响整个网络。因此，通过在整个网络的所有路由器上都配置合法 BSR 的地址范围，从而丢弃合法范围之外的自举报文，就可以防止此类攻击。

以上两种预防措施可以部分地保护网络中 BSR 的安全。但是如果某台合法的 BSR 路由器被攻击者控制，还是可能导致问题。

表1-22 配置 C-BSR

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
配置C-BSR	**c-bsr** *ipv6-address* [**scope** *scope-id*] [**hash-length** *hash-length* | **priority** *priority*] *	缺省情况下，没有配置C-BSR
（可选）配置合法的BSR地址范围	**bsr-policy** *acl6-number*	缺省情况下，BSR的地址范围不受任何限制

2. 配置BSR服务边界

BSR 作为 IPv6 双向 PIM 域中的管理核心，负责将收集到的 RP-Set 信息以自举报文的形式发向 IPv6 双向 PIM 域中的所有路由器。

BSR 的服务边界，即 IPv6 双向 PIM 域的边界。BSR 是针对特定的服务范围而言的，众多的 BSR 服务边界接口将网络划分成不同的 IPv6 双向 PIM 域，自举报文无法通过 IPv6 双向 PIM 域的边界，BSR 服务边界之外的路由器也不能参与本 IPv6 双向 PIM 域内的组播转发。

请在欲配置为 BSR 服务边界的路由器上进行如下配置。

表1-23 配置 BSR 服务边界

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置BSR的服务边界	**ipv6 pim bsr-boundary**	缺省情况下，没有配置BSR的服务边界

3. 关闭自举报文语义分片功能

BSR 周期性地向所在 IPv6 双向 PIM 域发送自举报文以通告 RP-Set 信息。当 RP-Set 信息较少时，自举报文被封装在一个 IPv6 报文中发送出去；而当 RP-Set 信息较多时，自举报文的大小可能超过接口的 MTU 值，从而触发其在 IP 层的分片。在这种情况下，一个 IP 分片的丢失就会导致整个自举报文都被丢弃。

自举报文语义分片功能可以解决上述问题：当自举报文大于接口 MTU 时，会被分解为多个自举报文分片。非 BSR 收到自举报文分片后，若发现某组范围对应的 RP 信息都在这一个分片中，便立即更新该组范围对应的 RP-Set；若发现某组范围映射的 RP 信息被分在了多个分片中，则待收齐了这些分片后再更新该组范围对应的 RP-Set。这样，由于不同分片所含组范围对应的 RP 信息不同，因此个别分片的丢失只影响该分片所含组范围对应的 RP 信息，而不会导致整个自举报文都被丢弃。

自举报文语义分片功能是缺省使能的，但由于不支持该功能的设备会将自举报文分片当作完整的自举报文处理，从而导致其学到的 RP-Set 信息不完整，因此当 IPv6 双向 PIM 域中存在此类设备时，请在已配置为 C-BSR 的路由器上关闭本功能。

表1-24 关闭自举报文语义分片功能

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
关闭自举报文语义分片功能	**undo bsm-fragment enable**	缺省情况下，自举报文语义分片功能处于使能状态

说明

通常，BSR 根据其 BSR 接口的 MTU 值对自举报文进行语义分片；而对由于新学到 IPv6 PIM 邻居而触发的自举报文发送，则根据发送接口的 MTU 值进行语义分片。

1.5 配置IPv6 PIM-SSM

提示

IPv6 PIM-SSM 模型需要 MLDv2 的支持，因此应确保连接有接收者的 IPv6 PIM 路由器上使能了 MLDv2。

1.5.1 IPv6 PIM-SSM配置任务简介

表1-25 IPv6 PIM-SSM 配置任务简介

配置任务	说明	详细配置
使能IPv6 PIM-SM	必选	1.5.3
配置IPv6 SSM组播组范围	可选	表1-26
配置IPv6 PIM公共特性	可选	1.6

1.5.2 配置准备

在配置 IPv6 PIM-SSM 之前，需完成以下任务：

- 配置任一 IPv6 单播路由协议，实现域内网络层互通

1.5.3 使能PIM-SM

提示

同一台设备相同实例的所有接口上启用的 IPv6 PIM 模式必须相同。

在进行各项 IPv6 PIM 配置之前，必须先使能 IPv6 组播路由。

由于 IPv6 PIM-SSM 是通过 IPv6 PIM-SM 的部分子集功能实现的，因此在配置 IPv6 PIM-SSM 之前须先使能 IPv6 PIM-SM。在部署 IPv6 PIM-SSM 域时，建议在其所有非边界接口上均使能 IPv6 PIM-SM。

表1-26 使能 IPv6 PIM-SM

操作	命令	说明
进入系统视图	**system-view**	-
使能IPv6组播路由，并进入IPv6 MRIB视图	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	缺省情况下，IPv6组播路由处于关闭状态 本命令的详细介绍请参见“IP组播命令参考”中的“IPv6组播路由与转发”
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能IPv6 PIM-SM	**ipv6 pim sm**	缺省情况下，IPv6 PIM-SM处于关闭状态

1.5.4 配置IPv6 SSM组播组范围

在把来自 IPv6 组播源的信息传递给接收者的过程中，是采用 IPv6 PIM-SSM 模型还是 IPv6 PIM-SM 模型，这取决于接收者订阅通道（S，G）中的 IPv6 组播组是否在 IPv6 SSM 组播组范围之内，所有使能了 IPv6 PIM-SM 的接口将会认为属于该范围内的 IPv6 组播组采用了 IPv6 PIM-SSM 模型。请在 IPv6 PIM-SSM 域内的所有路由器上进行如下配置。

提示

- 应确保 IPv6 PIM-SSM 域内所有路由器上配置的 IPv6 SSM 组播组地址范围都一致，否则 IPv6 组播信息将无法通过 SSM 模型进行传输。
- 如果某 IPv6 组播组属于 IPv6 SSM 组播组范围，但该组成员使用 MLDv1 发送加入报文，则设备不会触发（*，G）加入报文。

表1-27 配置 IPv6 SSM 组播组范围

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim**	-

操作	命令	说明
配置IPv6 SSM组播组的范围	**ssm-policy** *acl6-number*	缺省情况下，IPv6 SSM组播组的范围为FF3x::/32，其中x表示任意合法的scope

1.6 配置IPv6 PIM公共特性

1.6.1 IPv6 PIM公共特性配置任务简介

表1-28 IPv6 PIM 公共特性配置任务简介

配置任务	说明	详细配置
配置IPv6组播数据过滤器	可选	1.6.3
配置Hello报文过滤器	可选	1.6.4
配置Hello报文选项	可选	1.6.5
配置IPv6 PIM公共定时器	可选	1.6.6
配置加入/剪枝报文规格	可选	1.6.7
配置IPv6 PIM与BFD联动	可选	1.6.8
开启IPv6 PIM告警功能	可选	1.6.9

1.6.2 配置准备

在配置 IPv6 PIM 公共特性之前，需完成以下任务：

- 配置任一 IPv6 单播路由协议，实现域内网络层互通
- 配置 IPv6 PIM-DM 或 IPv6 PIM-SM

1.6.3 配置IPv6 组播数据过滤器

无论在 IPv6 PIM-DM 还是 IPv6 PIM-SM 域内，各路由器都可以对流经自己的 IPv6 组播数据进行检查，通过比较是否符合过滤规则来决定是否继续转发 IPv6 组播数据。也就是说 IPv6 PIM 域内的路由器能够成为 IPv6 组播数据的过滤器。过滤器的存在一方面有助于实现信息流量控制，另一方面可以在安全性方面限定下游接收者能够获得的信息。过滤器不仅过滤独立的 IPv6 组播数据，还过滤封装在注册报文中的 IPv6 组播数据。

通常，过滤器的位置距离 IPv6 组播源越近，过滤影响越明显。

表1-29 配置 IPv6 组播数据过滤器

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-

操作	命令	说明
配置IPv6组播数据过滤器	**source-policy** *acl6-number*	缺省情况下，没有配置IPv6组播数据过滤器

1.6.4 配置Hello报文过滤器

随着 IPv6 PIM 协议的推广和应用，对其安全性的要求也越来越高。建立正确的 IPv6 PIM 邻居是 IPv6 PIM 协议安全应用的前提。如果在接口上指定了合法 Hello 报文的源地址范围，便能够保证 IPv6 PIM 邻居的正确建立，从而有效防止各种 IPv6 PIM 协议报文攻击，提高设备对 IPv6 PIM 协议报文处理的安全性。

表1-30 配置 Hello 报文过滤器

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置合法Hello报文的源地址范围	**ipv6 pim neighbor-policy** *acl6-number*	缺省情况下，Hello报文的源地址范围不受任何限制


说明

当 Hello 报文过滤器的配置生效后，对于之前已建立的 IPv6 PIM 邻居，若由于其 Hello 报文被过滤而导致无法收到后续的 Hello 报文，将会在老化超时后被自动删除。

1.6.5 配置Hello报文选项

无论在 IPv6 PIM-DM 域还是在 IPv6 PIM-SM 域内，各路由器之间发送的 Hello 报文都包含很多可供配置的选项，对各选项的介绍如下：

- DR_Priority（仅用于 IPv6 PIM-SM）：表示竞选 DR 的优先级，优先级高的设备被选举为 DR。可以在与 IPv6 组播源或接收者直连的共享网络中的所有路由器上都配置此参数。
- Holdtime：表示保持 IPv6 PIM 邻居可达状态的时间，若超时后仍没有收到 Hello 报文，则认为 IPv6 PIM 邻居失效或不可达。
- LAN_Prune_Delay：表示在共享网络上传递剪枝报文的延迟时间，该选项由三部分组成：LAN-delay（发送剪枝报文的延迟时间）、Override-interval（剪枝否决时间）和禁止加入报文抑制能力。

LAN-delay 表示路由器从收到下游路由器发来的剪枝报文到继续向上游路由器发送剪枝报文的延迟时间，Override-interval 则表示允许下游路由器否决剪枝动作的时间，当共享网段内各 IPv6 PIM 路由器的 LAN-delay 或 Override-interval 不同时，取其中最大的值。路由器在收到下游路由器发来的剪枝报文后并不立即执行剪枝动作，而是仍将当前的转发状态保持 LAN-delay＋Override-interval 时间。如果下游路由器需要继续接收 IPv6 组播数据，则必须在 Override-interval 时间内向上游路由

器发送加入报文以否决这个剪枝动作，这就称为剪枝否决；如果 Override-interval 时间超时后未收到任何加入报文，上游路由器就会在 LAN-delay＋Override-interval 时间超时后执行剪枝动作。

通过在上游邻居上使能跟踪下游邻居的功能（即关闭加入报文抑制能力），可以记录已发送了加入报文且加入状态尚未超时的下游邻居的信息。使能该功能时，应在共享网段的所有 IPv6 PIM 路由器上都使能，否则上游邻居无法跟踪每个下游邻居的加入报文。

在接口上使能 IPv6 PIM 后，路由器会生成一个随机数作为 Hello 报文中的 Generation ID。一台 IPv6 PIM 路由器的 Generation ID 一般不会改变，除非其状态更新才会生成新的 Generation ID。这样，当 IPv6 PIM 路由器发现来自上游邻居的 Hello 报文中的 Generation ID 发生改变时，便认为上游邻居的状态发生了改变，从而触发发送加入报文以进行状态刷新。通过在接口上配置拒绝无 Generation ID 的 Hello 报文，可以实时了解上游邻居的状态。

对于既可在 IPv6 PIM 视图又可在接口视图下进行的配置来说，前者对所有接口都生效，而后者只对当前接口生效，但后者的配置优先级较高。

1. 全局配置Hello报文选项

表1-31 全局配置 Hello 报文选项

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
配置竞选DR的优先级	**hello-option dr-priority** *priority*	缺省情况下，竞选DR的优先级为1
配置保持IPv6 PIM邻居可达状态的时间	**hello-option holdtime** *time*	缺省情况下，保持IPv6 PIM邻居可达状态的时间为105秒
配置发送剪枝报文的延迟时间	**hello-option lan-delay** *delay*	缺省情况下，发送剪枝报文的延迟时间为500毫秒
配置剪枝否决时间	**hello-option override-interval** *interval*	缺省情况下，剪枝否决时间为2500毫秒
使能邻居跟踪功能	**hello-option neighbor-tracking**	缺省情况下，邻居跟踪功能处于关闭状态

2. 在接口上配置Hello报文选项

表1-32 在接口上配置 Hello 报文选项

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置竞选DR的优先级	**ipv6 pim hello-option dr-priority** *priority*	缺省情况下，竞选DR的优先级为1
配置保持IPv6 PIM邻居可达状态的时间	**ipv6 pim hello-option holdtime** *time*	缺省情况下，保持IPv6 PIM邻居可达状态的时间为105秒
配置发送剪枝报文的延迟时间	**ipv6 pim hello-option lan-delay** *delay*	缺省情况下，发送剪枝报文的延迟时间为500毫秒

操作	命令	说明
配置剪枝否决时间	**ipv6 pim hello-option override-interval** *interval*	缺省情况下，剪枝否决时间为2500毫秒
使能邻居跟踪功能	**ipv6 pim hello-option neighbor-tracking**	缺省情况下，邻居跟踪功能处于关闭状态
配置拒绝无Generation ID的Hello报文	**ipv6 pim require-genid**	缺省情况下，接受无Generation ID的Hello报文

1.6.6 配置IPv6 PIM公共定时器

提示

- 如果对网络没有特殊要求，各定时器的值建议采用缺省值。
- IPv6 PIM 接口向上游邻居发送加入/剪枝报文的时间间隔必须小于加入/剪枝状态的保持时间，以免上游邻居老化超时。

IPv6 PIM 路由器通过周期性地发送 Hello 报文，以发现 IPv6 PIM 邻居，并维护各路由器之间的 IPv6 PIM 邻居关系。

为了避免多个 IPv6 PIM 路由器同时发送 Hello 报文而导致冲突，当 IPv6 PIM 路由器在收到新邻居发来的 Hello 报文时，将延迟一段时间后再发送 Hello 报文，该时间值为小于“触发 Hello 报文的最大延迟时间”的一个随机值。

IPv6 PIM 路由器通过周期性地向其上游路由器发送加入/剪枝报文以更新状态，在该报文中携带有保持时间，上游路由器为被剪枝的下游接口设置加入/剪枝状态保持定时器。

当路由器没有收到来自 IPv6 组播源 S 的后续 IPv6 组播数据时，不会立即删除（S，G）表项，而是将其维持一段时间后再删除，这段时间就称为 IPv6 组播源的生存时间。

对于既可在 IPv6 PIM 视图又可在接口视图下进行的配置来说，前者对所有接口都生效，而后者只对当前接口生效，但后者的配置优先级较高。

1. 全局配置IPv6 PIM公共定时器

表1-33 全局配置 IPv6 PIM 公共定时器

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
配置发送Hello报文的时间间隔	**timer hello** *interval*	缺省情况下，发送Hello报文的时间间隔为30秒
配置发送加入/剪枝报文的时间间隔	**timer join-prune** *interval*	缺省情况下，发送加入/剪枝报文的时间间隔为60秒 本命令不会立即生效，新配置的发送间隔将在当前发送间隔完成后生效

操作	命令	说明
配置加入/剪枝状态的保持时间	**holdtime join-prune** *time*	缺省情况下，加入/剪枝状态的保持时间为210秒
配置IPv6组播源生存时间	**source-lifetime** *time*	缺省情况下，IPv6组播源的生存时间为210秒

2. 在接口上配置IPv6 PIM公共定时器

表1-34 在接口上配置 IPv6 PIM 公共定时器

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置发送Hello报文的时间间隔	**ipv6 pim timer hello** *interval*	缺省情况下，发送Hello报文的时间间隔为30秒
配置触发Hello报文的最大延迟时间	**ipv6 pim triggered-hello-delay** *delay*	缺省情况下，触发Hello报文的最大延迟时间为5秒
配置发送加入/剪枝报文的时间间隔	**ipv6 pim timer join-prune** *interval*	缺省情况下，发送加入/剪枝报文的时间间隔为60秒 本命令不会立即生效，新配置的发送间隔将在当前发送间隔完成后生效
配置加入/剪枝状态的保持时间	**ipv6 pim holdtime join-prune** *time*	缺省情况下，加入/剪枝状态的保持时间为210秒

1.6.7 配置加入/剪枝报文规格

如果加入/剪枝报文的尺寸较大，则丢失一个报文将导致较多信息的遗失；如果加入/剪枝报文的尺寸较小，则单个报文的丢失所产生的影响也将降低。

表1-35 配置加入/剪枝报文规格

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6 PIM视图	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	-
配置加入/剪枝报文的最大长度	**jp-pkt-size** *size*	缺省情况下，加入/剪枝报文的最大长度为8100字节

1.6.8 配置IPv6 PIM与BFD联动

提示

只有在接口上先使能了 IPv6 PIM-DM 或 IPv6 PIM-SM，本配置才能生效。

IPv6 PIM 借助 Hello 报文在共享网段中选举出 DR，使其成为该网段中组 IPv6 播数据的唯一转发者。当 DR 出现故障时，只有待其老化后才会触发新的 DR 选举过程，这个过程通常比较长。为了实现 DR 的快速切换，可以在共享网段的 IPv6 PIM 邻居之间引入 BFD（Bidirectional Forwarding Detection，双向转发检测）机制进行链路状态的快速检测。通过在共享网段内的所有 IPv6 PIM 路由器上都使能 IPv6 PIM 与 BFD 联动功能，可以使这些 IPv6 PIM 邻居快速感知 DR 故障并重新选举 DR。有关 BFD 的详细介绍，请参见“可靠性配置指导”中的“BFD”。

表1-36 配置 IPv6 PIM 与 BFD 联动

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能IPv6 PIM与BFD联动功能	**ipv6 pim bfd enable**	缺省情况下，IPv6 PIM与BFD联动功能处于关闭状态

1.6.9 开启IPv6 PIM告警功能

开启了 IPv6 PIM 的告警功能之后，IPv6 PIM 会生成告警信息，以向网管软件报告本模块的重要事件。该信息将发送至 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

表1-37 开启 IPv6 PIM 告警功能

操作	命令	说明
进入系统视图	**system-view**	-
开启IPv6 PIM的告警功能	**snmp-agent trap enable pim6** [**candidate-bsr-win-election** | **elected-bsr-lost-election** | **neighbor-loss**] *	缺省情况下，IPv6 PIM的告警功能处于开启状态

1.7 IPv6 PIM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 的运行情况，通过查看显示信息验证配置的效果。

有关 **display interface register-tunnel** 命令的详细介绍，请参见“IP 组播命令参考”中的“PIM”。

表1-38 IPv6 PIM 显示和维护

操作	命令
显示Register-Tunnel接口的相关信息	**display interface** [**register-tunnel** [*interface-number*]] [**brief** [**description** | **down**]]
显示IPv6 PIM-SM域中的BSR信息	**display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **bsr-info**
显示IPv6 PIM所使用的路由信息	**display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **claimed-route** [*ipv6-source-address*]
显示IPv6 PIM-SM域中的C-RP信息	**display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **c-rp** [**local**]

操作	命令
显示IPv6双向PIM的DF信息	**display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **df-info** [*ipv6-rp-address*]
显示接口上的IPv6 PIM信息	**display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**verbose**]
显示IPv6 PIM邻居信息	**display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **neighbor** [*ipv6-neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *
显示IPv6 PIM路由表的内容	**display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **routing-table** [*ipv6-group-address* [*prefix-length*] | *ipv6-source-address* [*prefix-length*] | **flags** *flag-value* | **fsm** | **incoming-interface** *interface-type interface-number* | **mode** *mode-type* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *
显示IPv6 PIM-SM域中的RP的信息	**display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **rp-info** [*ipv6-group-address*]
显示IPv6 PIM协议报文的统计信息	**display ipv6 pim statistics**

1.8 IPv6 PIM典型配置举例

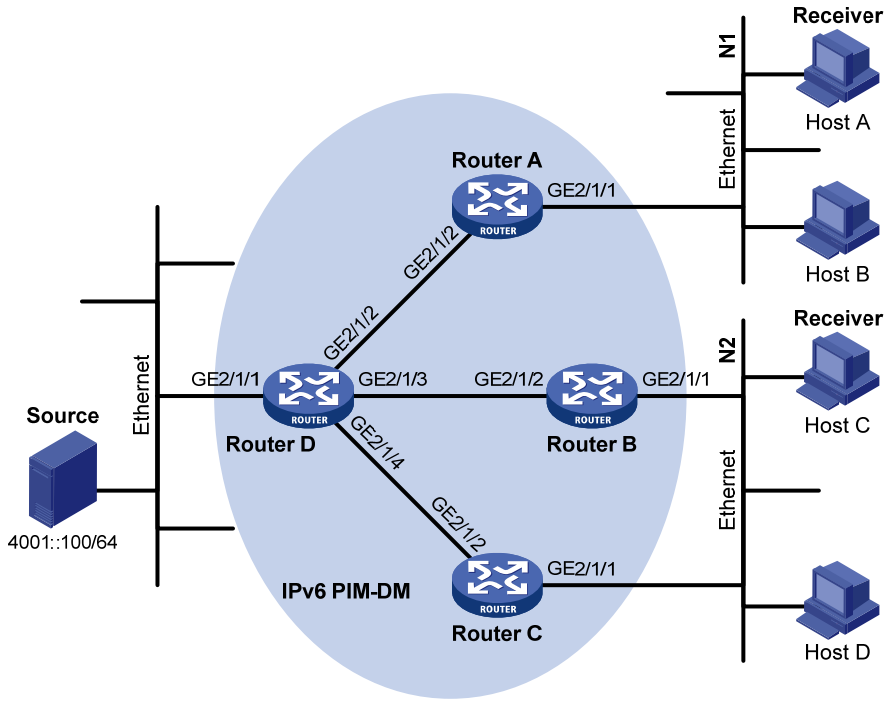
1.8.1 IPv6 PIM-DM典型配置举例

1. 组网需求

- 接收者通过组播方式接收视频点播信息，不同组织的接收者群体组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 IPv6 PIM 域采用 DM 方式。
- Host A 和 Host C 为两个末梢网络中的 IPv6 组播信息接收者；Router D 通过 GigabitEthernet2/1/1 接口与 IPv6 组播源（Source）所在的网络连接；Router A 通过 GigabitEthernet2/1/1 接口连接末梢网络 N1，通过 GigabitEthernet2/1/2 接口连接 Router D；Router B 和 Router C 分别通过各自的 GigabitEthernet2/1/1 接口连接末梢网络 N2，并分别通过各自的 GigabitEthernet2/1/2 接口连接 Router D。
- Router A 与末梢网络 N1 之间运行 MLDv1；Router B 和 Router C 与末梢网络 N2 之间也运行 MLDv1。

2. 组网图

图1-15 IPv6 PIM-DM 典型配置组网图



设备	接口	IPv6地址	设备	接口	IPv6地址
Router A	GE2/1/1	1001::1/64	Router D	GE2/1/1	4001::1/64
	GE2/1/2	1002::1/64		GE2/1/2	1002::2/64
Router B	GE2/1/1	2001::1/64		GE2/1/3	2002::2/64
	GE2/1/2	2002::1/64		GE2/1/4	3001::2/64
Router C	GE2/1/1	2001::2/64			
	GE2/1/2	3001::1/64			

3. 配置步骤

(1) 配置 IPv6 地址和 IPv6 单播路由协议

请按照 图 1-15 配置各接口的IPv6 地址和前缀长度，具体配置过程略。

配置 IPv6 PIM-DM 域内的各路由器之间采用 OSPFv3 协议进行互连，确保 IPv6 PIM-DM 域内部在网络层互通，并且各路由器之间能够借助 IPv6 单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IPv6 组播路由，并使能 IPv6 PIM-DM 和 MLD

在 Router A 上使能 IPv6 组播路由，在接口 GigabitEthernet2/1/2 上使能 IPv6 PIM-DM，并在其连接末梢网络的接口 GigabitEthernet2/1/1 上使能 MLD。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mld enable
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ipv6 pim dm
[RouterA-GigabitEthernet2/1/2] quit
```

Router B 和 Router C 的配置与 Router A 相似，配置过程略。

在 Router D 上使能 IPv6 组播路由，并在各接口上使能 IPv6 PIM-DM。

```
<RouterD> system-view
[RouterD] ipv6 multicast routing
[RouterD-mrib6] quit
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] ipv6 pim dm
[RouterD-GigabitEthernet2/1/1] quit
[RouterD] interface gigabitethernet 2/1/2
[RouterD-GigabitEthernet2/1/2] ipv6 pim dm
[RouterD-GigabitEthernet2/1/2] quit
[RouterD] interface gigabitethernet 2/1/3
[RouterD-GigabitEthernet2/1/3] ipv6 pim dm
[RouterD-GigabitEthernet2/1/3] quit
[RouterD] interface gigabitethernet 2/1/4
[RouterD-GigabitEthernet2/1/4] ipv6 pim dm
[RouterD-GigabitEthernet2/1/4] quit
```

2. 验证配置

通过使用 **display ipv6 pim interface** 命令可以查看路由器接口上 IPv6 PIM 的配置和运行情况。例如：

显示 Router D 上 IPv6 PIM 的配置信息。

```
[RouterD] display ipv6 pim interface
 Interface           NbrCnt HelloInt   DR-Pri    DR-Address
 GE2/1/1             0      30         1         FE80::A01:201:1
                                                 (local)
 GE2/1/2             0      30         1         FE80::A01:201:2
                                                 (local)
 GE2/1/3             1      30         1         FE80::A01:201:3
                                                 (local)
 GE2/1/4             1      30         1         FE80::A01:201:4
                                                 (local)
```

通过使用 **display ipv6 pim neighbor** 命令可以查看路由器之间的 IPv6 PIM 邻居关系。例如：

显示 Router D 上 IPv6 PIM 的邻居关系信息。

```
[RouterD] display ipv6 pim neighbor
 Total Number of Neighbors = 3

 Neighbor        Interface           Uptime   Expires  Dr-Priority
 FE80::A01:101:1 GE2/1/2             00:04:00 00:01:29 1
 FE80::B01:102:2 GE2/1/3             00:04:16 00:01:29 3
 FE80::C01:103:3 GE2/1/4             00:03:54 00:01:17 5
```

假如 Host A 需要接收 IPv6 组播组 G（FF0E::101）的信息，当 IPv6 组播源 S（4001::100/64）向 IPv6 组播组 G 发送 IPv6 组播数据时，通过扩散生成 SPT，SPT 路径中各路由器（Router A 和 Router D）上都存在（S，G）表项，Host A 向 Router A 发送 MLD 报告以加入 IPv6 组播组 G，在 Router A 上生成（*，G）表项。通过使用 **display ipv6 pim routing-table** 命令可以查看路由器的 IPv6 PIM 路由表信息。例如：

显示 Router A 上的 IPv6 PIM 路由表信息。

```
[RouterA] display ipv6 pim routing-table
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, FF0E::101)
     Protocol: pim-dm, Flag: WC
     UpTime: 00:01:24
     Upstream interface: NULL
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/1/1
             Protocol: mld, UpTime: 00:01:20, Expires: -

 (4001::100, FF0E::101)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:01:20
     Upstream interface: GigabitEthernet2/1/2
         Upstream neighbor: 1002::2
         RPF prime neighbor: 1002::2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/1/1
             Protocol: pim-dm, UpTime: 00:01:20, Expires: -
```

显示 Router D 上的 IPv6 PIM 路由表信息。

```
[RouterD] display ipv6 pim routing-table
 Total 0 (*, G) entry; 1 (S, G) entry

 (4001::100, FF0E::101)
     Protocol: pim-dm, Flag: LOC ACT
     UpTime: 00:02:19
     Upstream interface: GigabitEthernet2/1/1
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 2
         1: GigabitEthernet2/1/2
             Protocol: pim-dm, UpTime: 00:02:19, Expires: -
         2: GigabitEthernet2/1/4
             Protocol: pim-dm, UpTime: 00:02:19, Expires: -
```

1.8.2 IPv6 PIM-SM非管理域典型配置举例

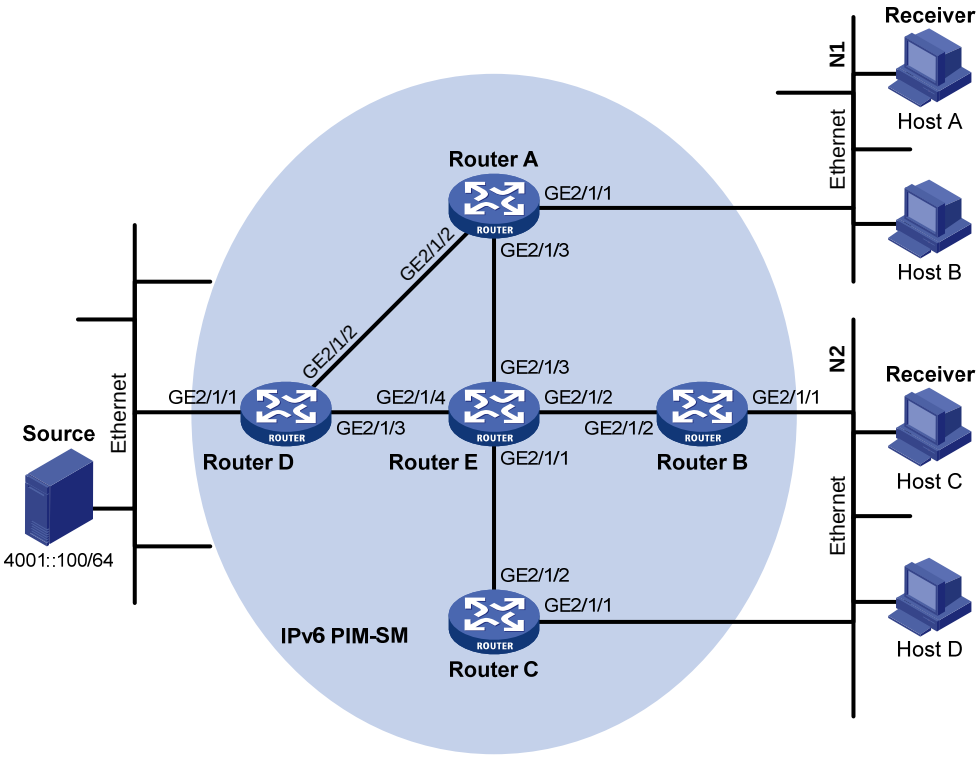
1. 组网需求

- 接收者通过组播方式接收视频点播信息，不同组织的接收者群体组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 IPv6 PIM 域采用 SM 非管理域方式。

- Host A 和 Host C 为两个末梢网络中的 IPv6 组播信息接收者；Router D 通过 GigabitEthernet2/1/1 接口与 IPv6 组播源（Source）所在网络连接；Router A 通过 GigabitEthernet2/1/1 接口连接末梢网络 N1，通过 GigabitEthernet2/1/2 接口和 GigabitEthernet2/1/3 接口分别连接 Router D 和 Router E；Router B 和 Router C 分别通过各自的 GigabitEthernet2/1/1 接口连接末梢网络 N2，并分别通过各自的 GigabitEthernet2/1/2 接口连接 Router E。
- 将 Router E 的 GigabitEthernet2/1/3 接口配置为 C-BSR 和 C-RP，其中 C-RP 所服务的 IPv6 组播组范围为 FF0E::101/64；在所有路由器上将 Router D 的 GigabitEthernet2/1/2 接口配置为静态 RP，以对动态 RP 进行备份。
- Router A 与末梢网络 N1 之间运行 MLDv1；Router B 和 Router C 与末梢网络 N2 之间也运行 MLDv1。

2. 组网图

图1-16 IPv6 PIM-SM 非管理域典型配置组网图



设备	接口	IPv6地址	设备	接口	IPv6地址
Router A	GE2/1/1	1001::1/64	Router D	GE2/1/1	4001::1/64
	GE2/1/2	1002::1/64		GE2/1/2	1002::2/64
	GE2/1/3	1003::1/64		GE2/1/3	4002::1/64
Router B	GE2/1/1	2001::1/64	Router E	GE2/1/1	3001::2/64
	GE2/1/2	2002::1/64		GE2/1/2	2002::2/64
Router C	GE2/1/1	2001::2/64		GE2/1/3	1003::2/64
	GE2/1/2	3001::1/64		GE2/1/4	4002::2/64

3. 配置步骤

(1) 配置 IPv6 地址和 IPv6 单播路由协议

请按照 图 1-16 配置各接口的IPv6 地址和前缀长度，具体配置过程略。

配置 IPv6 PIM-SM 域内的各路由器之间采用 OSPFv3 协议进行互连，确保 IPv6 PIM-SM 域内部在网络层互通，并且各路由器之间能够借助 IPv6 单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IPv6 组播路由，并使能 IPv6 PIM-SM 和 MLD

在 Router A 上使能 IPv6 组播路由，在其连接末梢网络的接口 GigabitEthernet2/1/1 上使能 MLD，并在其它接口上使能 IPv6 PIM-SM。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mld enable
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ipv6 pim sm
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] interface gigabitethernet 2/1/3
[RouterA-GigabitEthernet2/1/3] ipv6 pim sm
[RouterA-GigabitEthernet2/1/3] quit
```

Router B 和 Router C 的配置与 Router A 相似，Router D 和 Router E 除了不需要在相应接口上使能 MLD 外，其它的配置也与 Router A 相似，配置过程略。

(3) 配置 C-BSR、C-RP 和静态 RP

在 Router E 上配置 RP 通告的服务范围，以及 C-BSR 和 C-RP 的位置，并指定静态 RP。

```
<RouterE> system-view
[RouterE] acl ipv6 number 2005
[RouterE-acl6-basic-2005] rule permit source ff0e::101 64
[RouterE-acl6-basic-2005] quit
[RouterE] ipv6 pim
[RouterE-pim6] c-bsr 1003::2
[RouterE-pim6] c-rp 1003::2 group-policy 2005
[RouterE-pim6] static-rp 1002::2
[RouterE-pim6] quit
```

在 Router A 上配置静态 RP。

```
[RouterA] ipv6 pim
[RouterA-pim6] static-rp 1002::2
[RouterA-pim6] quit
```

Router B、Router C 和 Router D 的配置与 Router A 相似，配置过程略。

4. 验证配置

通过使用 **display ipv6 pim interface** 命令可以查看接口上的 IPv6 PIM 信息。例如：

显示 Router A 的接口上的 IPv6 PIM 信息。

```
[RouterA] display ipv6 pim interface
 Interface            NbrCnt HelloInt   DR-Pri    DR-Address
 GE2/1/1              0      30         1         FE80::A01:201:1
                                                  (local)
 GE2/1/2              1      30         1         FE80::A01:201:2
 GE2/1/3              1      30         1         FE80::A01:201:2
```

通过使用 **display ipv6 pim bsr-info** 命令可以查看 IPv6 PIM-SM 域中的 BSR 信息。例如：

显示 Router A 上 IPv6 PIM-SM 域中的 BSR 信息。

```
[RouterA] display ipv6 pim bsr-info
 Scope: non-scoped
      State: Accept Preferred
      Bootstrap timer: 00:01:44
      Elected BSR address: 1003::2
        Priority: 64
        Hash mask length: 126
        Uptime: 00:11:18
```

显示 Router E 上 IPv6 PIM-SM 域中的 BSR 信息。

```
[RouterE] display ipv6 pim bsr-info
 Scope: non-scoped
      State: Elected
      Bootstrap timer: 00:01:44
      Elected BSR address: 1003::2
        Priority: 64
        Hash mask length: 126
        Uptime: 00:11:18
      Candidate BSR address: 1003::2
        Priority: 64
        Hash mask length: 126
```

通过使用 **display ipv6 pim rp-info** 命令可以查看 IPv6 PIM-SM 域中的 RP 信息。例如：

显示 Router A 上所有 IPv6 组播组对应的 RP 信息。

```
[RouterA] display ipv6 pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: FF0E::101/64
       RP address               Priority  HoldTime  Uptime    Expires
       1003::2                  192       150       00:05:19  00:02:11

Static RP information:
       RP address               ACL   Mode    Preferred
       1002::2                  ----  pim-sm  No
```

1.8.3 IPv6 PIM-SM管理域典型配置举例

1. 组网需求

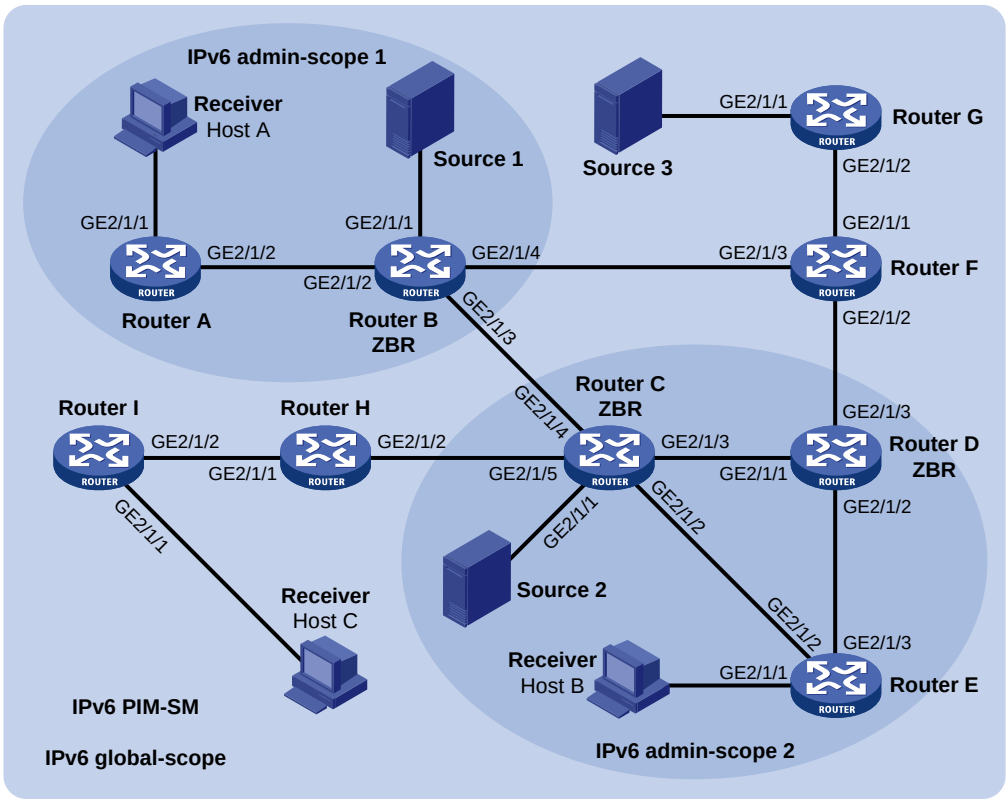
- 接收者通过组播方式接收视频点播信息，整个 IPv6 PIM 域采用 SM 管理域方式，划分为 IPv6 管理域 1（Scope 值为 4）、IPv6 管理域 2（Scope 值为 4）和 IPv6 Global 域（Scope 值为 14），Router B、Router C 和 Router D 为各 IPv6 管理域的 ZBR。
- Source 1 和 Source 2 分别向 IPv6 组播组 FF14::101 发送内容不同的 IPv6 组播信息，Host A 和 Host B 则分别只接收来自 Source 1 和 Source 2 的 IPv6 组播信息；Source 3 向 IPv6 组播组 FF1E::202 发送 IPv6 组播信息，Host C 为其接收者。
- Router B 的 GigabitEthernet2/1/2 接口为 IPv6 管理域 1 的 C-BSR 和 C-RP，服务于 Scope 值为 4 的 IPv6 组播组；Router D 的 GigabitEthernet2/1/1 接口为 IPv6 管理域 2 的 C-BSR 和

C-RP，服务于 Scope 值为 4 的 IPv6 组播组；Router F 的 GigabitEthernet2/1/1 接口为 IPv6 Global 域的 C-BSR 和 C-RP，服务于 Scope 值为 14 的 IPv6 组播组。

- Router A、Router E 和 Router I 分别与各自所连接的接收者之间运行 MLDv1。

2. 组网图

图1-17 IPv6 PIM-SM 管理域配置组网图



设备	接口	IPv6地址	设备	接口	IPv6地址
Router A	GE2/1/1	1001::1/64	Router D	GE2/1/1	3003::2/64
	GE2/1/2	1002::1/64		GE2/1/3	6001::1/64
Router B	GE2/1/1	2001::1/64		GE2/1/3	6002::1/64
	GE2/1/2	1002::2/64	Router E	GE2/1/1	7001::1/64
	GE2/1/3	2002::1/64		GE2/1/2	3002::2/64
	GE2/1/4	2003::1/64		GE2/1/3	6001::2/64
Router C	GE2/1/1	3001::1/64	Router F	GE2/1/1	8001::1/64
	GE2/1/2	3002::1/64		GE2/1/2	6002::2/64
	GE2/1/3	3003::1/64		GE2/1/3	2003::2/64
	GE2/1/4	2002::2/64	Router G	GE2/1/1	9001::1/64
	GE2/1/5	3004::1/64		GE2/1/2	8001::2/64
Router H	GE2/1/1	4001::1/64	Source 1	-	2001::100/64
	GE2/1/2	3004::2/64	Source 2	-	3001::100/64
Router I	GE2/1/1	5001::1/64	Source 3	-	9001::100/64
	GE2/1/2	4001::2/64			

3. 配置步骤

(1) 配置 IPv6 地址和 IPv6 单播路由协议

请按照 图 1-17 配置各接口的IPv6 地址和前缀长度，具体配置过程略。

配置 IPv6 PIM-SM 域内的各路由器之间采用 OSPFv3 协议进行互连，确保 IPv6 PIM-SM 域内部在网络层互通，并且各路由器之间能够借助 IPv6 单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IPv6 组播路由和 IPv6 管理域机制，并使能 IPv6 PIM-SM 和 MLD

在 Router A 上使能 IPv6 组播路由，在接口 GigabitEthernet2/1/2 上使能 IPv6 PIM-SM，并在其连接有接收者的接口 GigabitEthernet2/1/1 上使能 MLD。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mld enable
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ipv6 pim sm
[RouterA-GigabitEthernet2/1/2] quit
```

Router E 和 Router I 的配置与 Router A 相似，配置过程略。

在 Router B 上使能 IPv6 组播路由，并在各接口上使能 IPv6 PIM-SM。

```
<RouterB> system-view
[RouterB] ipv6 multicast routing
[RouterB-mrib6] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ipv6 pim sm
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] ipv6 pim sm
[RouterB-GigabitEthernet2/1/2] quit
[RouterB] interface gigabitethernet 2/1/3
[RouterB-GigabitEthernet2/1/3] ipv6 pim sm
[RouterB-GigabitEthernet2/1/3] quit
[RouterB] interface gigabitethernet 2/1/4
[RouterB-GigabitEthernet2/1/4] ipv6 pim sm
[RouterB-GigabitEthernet2/1/4] quit
```

Router C、Router D、Router F、Router G 和 Router H 的配置与 Router B 相似，配置过程略。

(3) 配置 IPv6 管理域边界

在 Router B 上将接口 GigabitEthernet2/1/3 和 GigabitEthernet2/1/4 配置为 IPv6 管理域 1 的边界。

```
[RouterB] interface gigabitethernet 2/1/3
[RouterB-GigabitEthernet2/1/3] ipv6 multicast boundary scope 4
[RouterB-GigabitEthernet2/1/3] quit
[RouterB] interface gigabitethernet 2/1/4
[RouterB-GigabitEthernet2/1/4 ipv6 multicast boundary scope 4
[RouterB-GigabitEthernet2/1/4] quit
```

在 Router C 上将接口 GigabitEthernet2/1/4 和 GigabitEthernet2/1/5 配置为 IPv6 管理域 2 的边界。

```
<RouterC> system-view
[RouterC] interface gigabitethernet 2/1/4
[RouterC-GigabitEthernet2/1/4] ipv6 multicast boundary scope 4
[RouterC-GigabitEthernet2/1/4] quit
[RouterC] interface gigabitethernet 2/1/5
[RouterC-GigabitEthernet2/1/5] ipv6 multicast boundary scope 4
[RouterC-GigabitEthernet2/1/5] quit
```

在 Router D 上将接口 GigabitEthernet2/1/3 配置为 IPv6 管理域 2 的边界。

```
<RouterD> system-view
[RouterD] interface gigabitethernet 2/1/3
[RouterD-GigabitEthernet2/1/3] ipv6 multicast boundary scope 4
[RouterD-GigabitEthernet2/1/3] quit
```

(4) 配置 C-BSR 和 C-RP

在 Router B 上配置 RP 通告的服务范围，并将接口 GigabitEthernet2/1/2 配置为 IPv6 管理域 1 的 C-BSR 和 C-RP。

```
[RouterB] ipv6 pim
[RouterB-pim6] c-bsr 1002::2 scope 4
[RouterB-pim6] c-rp 1002::2 scope 4
[RouterB-pim6] quit
```

在 Router D 上配置 RP 通告的服务范围，并将接口 GigabitEthernet2/1/1 配置为 IPv6 管理域 2 的 C-BSR 和 C-RP。

```
[RouterD] ipv6 pim
[RouterD-pim6] c-bsr 3003::2 scope 4
[RouterD-pim6] c-rp 3003::2 scope 4
[RouterD-pim6] quit
```

在 Router F 上将接口 GigabitEthernet2/1/1 配置为 IPv6 Global 域的 C-BSR 和 C-RP。

```
<RouterF> system-view
[RouterF] ipv6 pim
[RouterF-pim6] c-bsr 8001::1
[RouterF-pim6] c-rp 8001::1
[RouterF-pim6] quit
```

4. 验证配置

通过使用 **display ipv6 pim bsr-info** 命令可以查看 IPv6 PIM-SM 域中的 BSR 信息。例如：

显示 Router B 上 IPv6 PIM-SM 域中的 BSR 信息。

```
[RouterB] display ipv6 pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:25
     Elected BSR address: 8001::1
       Priority: 64
       Hash mask length: 126
       Uptime: 00:01:45

 Scope: 4
     State: Elected
     Bootstrap timer: 00:00:06
     Elected BSR address: 1002::2
       Priority: 64
       Hash mask length: 126
       Uptime: 00:04:54
     Candidate BSR address: 1002::2
       Priority: 64
       Hash mask length: 126
```

显示 Router D 上 IPv6 PIM-SM 域中的 BSR 信息。

```
[RouterD] display ipv6 pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:25
     Elected BSR address: 8001::1
       Priority: 64
       Hash mask length: 126
       Uptime: 00:01:45

 Scope: 4
     State: Elected
     Bootstrap timer: 00:01:25
     Elected BSR address: 3003::2
       Priority: 64
       Hash mask length: 126
       Uptime: 00:01:45
     Candidate BSR address: 3003::2
       Priority: 64
       Hash mask length: 126
```

显示 Router F 上 IPv6 PIM-SM 域中的 BSR 信息。

```
[RouterF] display ipv6 pim bsr-info
 Scope: non-scoped
     State: Elected
     Bootstrap timer: 00:00:49
     Elected BSR address: 8001::1
       Priority: 64
       Hash mask length: 126
       Uptime: 00:01:11
     Candidate BSR address: 8001::1
       Priority: 64
       Hash mask length: 126
```

通过使用 **display ipv6 pim rp-info** 命令可以查看 IPv6 PIM-SM 域中的 RP 信息。例如：

显示 Router B 上所有 IPv6 组播组对应的 RP 信息。

```
[RouterB] display ipv6 pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: FF00::/8
       RP address               Priority  HoldTime  Uptime    Expires
       8001::1                  192       180       00:01:14  00:02:46
   Scope: 4
     Group/MaskLen: FF04::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FF14::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
```

```
    Group/MaskLen: FF24::/16
      RP address               Priority  HoldTime  Uptime    Expires
      1002::2 (local)          192       180       00:02:03  00:02:56
    Group/MaskLen: FF34::/16
      RP address               Priority  HoldTime  Uptime    Expires
      1002::2 (local)          192       180       00:02:03  00:02:56
    Group/MaskLen: FF44::/16
      RP address               Priority  HoldTime  Uptime    Expires
      1002::2 (local)          192       180       00:02:03  00:02:56
    Group/MaskLen: FF54::/16
      RP address               Priority  HoldTime  Uptime    Expires
      1002::2 (local)          192       180       00:02:03  00:02:56
    Group/MaskLen: FF64::/16
      RP address               Priority  HoldTime  Uptime    Expires
      1002::2 (local)          192       180       00:02:03  00:02:56
    Group/MaskLen: FF74::/16
      RP address               Priority  HoldTime  Uptime    Expires
      1002::2 (local)          192       180       00:02:03  00:02:56
    Group/MaskLen: FF84::/16
      RP address               Priority  HoldTime  Uptime    Expires
      1002::2 (local)          192       180       00:02:03  00:02:56
    Group/MaskLen: FF94::/16
      RP address               Priority  HoldTime  Uptime    Expires
      1002::2 (local)          192       180       00:02:03  00:02:56
    Group/MaskLen: FFA4::/16
      RP address               Priority  HoldTime  Uptime    Expires
      1002::2 (local)          192       180       00:02:03  00:02:56
    Group/MaskLen: FFB4::/16
      RP address               Priority  HoldTime  Uptime    Expires
      1002::2 (local)          192       180       00:02:03  00:02:56
    Group/MaskLen: FFC4::/16
      RP address               Priority  HoldTime  Uptime    Expires
      1002::2 (local)          192       180       00:02:03  00:02:56
    Group/MaskLen: FFD4::/16
      RP address               Priority  HoldTime  Uptime    Expires
      1002::2 (local)          192       180       00:02:03  00:02:56
    Group/MaskLen: FFE4::/16
      RP address               Priority  HoldTime  Uptime    Expires
      1002::2 (local)          192       180       00:02:03  00:02:56
    Group/MaskLen: FFF4::/16
      RP address               Priority  HoldTime  Uptime    Expires
      1002::2 (local)          192       180       00:02:03  00:02:56
    Group/MaskLen: FF04::/16
      RP address               Priority  HoldTime  Uptime    Expires
      1002::2 (local)          192       180       00:02:03  00:02:56
```

显示 Router F 上所有 IPv6 组播组对应的 RP 信息。

```
[RouterF] display ipv6 pim rp-info
 BSR RP information:
```

```
Scope: non-scoped
  Group/MaskLen: FF00::/8
    RP address                Priority  HoldTime  Uptime    Expires
    8001::1 (local)           192       180       00:10:28  00:02:31
```

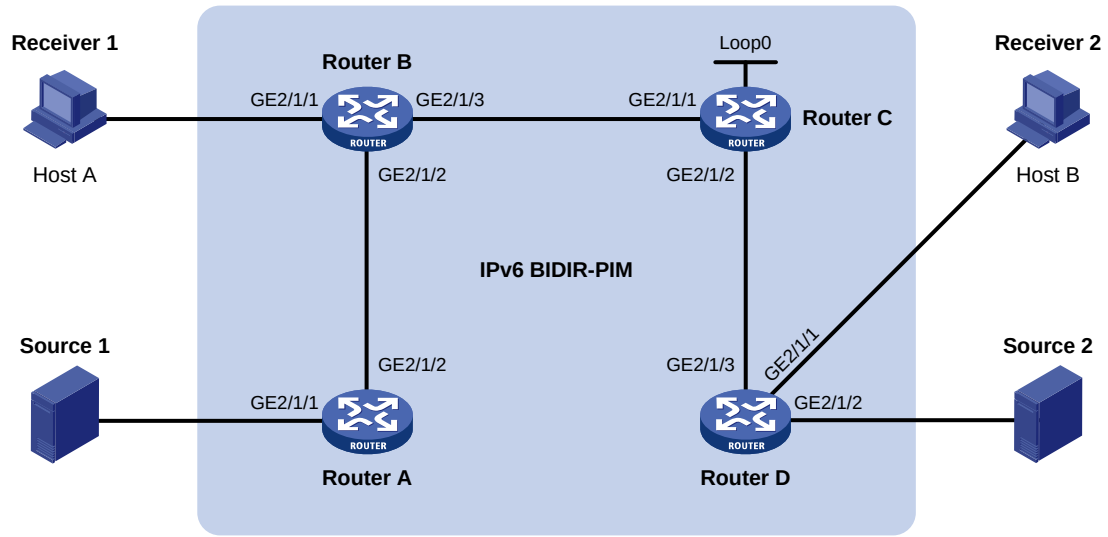
1.8.4 IPv6 双向PIM典型配置举例

1. 组网需求

- 整个 IPv6 PIM 域采用 BIDIR 方式，Source 1 和 Source 2 都向 IPv6 组播组 FF14::101 发送 IPv6 组播信息，Host A 和 Host B 为 IPv6 组播信息的接收者。
- 将 Router C 的 GigabitEthernet2/1/1 接口配置为 C-BSR，Loopback0 接口配置为服务于 IPv6 双向 PIM 的 C-RP。
- Router B 和 Router D 分别与各自所连接的接收者之间运行 MLDv1。

2. 组网图

图1-18 IPv6 双向 PIM 典型配置组网图



设备	接口	IPv6地址	设备	接口	IPv6地址
Router A	GE2/1/1	1001::1/64	Router D	GE2/1/1	4001::1/64
	GE2/1/2	1002::1/64		GE2/1/2	5001::1/64
Router B	GE2/1/1	2001::1/64		GE2/1/3	3001::2/64
	GE2/1/2	1002::2/64	Source 1	-	1001::2/64
	GE2/1/3	2002::1/64	Source 2	-	5001::2/64
Router C	GE2/1/1	2002::2/64	Receiver 1	-	2001::2/64
	GE2/1/2	3001::1/64	Receiver 2	-	4001::2/64
	Loop0	6001::1/128			

3. 配置步骤

(1) 配置 IPv6 地址和 IPv6 单播路由协议

请按照 图 1-18 配置各接口的IPv6 地址和前缀长度，具体配置过程略。

配置 IPv6 双向 PIM 域内的各路由器之间采用 OSPFv3 协议进行互连，确保 IPv6 双向 PIM 域内部在网络层互通，并且各路由器之间能够借助 IPv6 单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IPv6 组播路由，并使能 IPv6 PIM-SM、IPv6 双向 PIM 和 MLD

在 Router A 上使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-SM，并使能 IPv6 双向 PIM。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ipv6 pim sm
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ipv6 pim sm
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] ipv6 pim
[RouterA-pim6] bidir-pim enable
[RouterA-pim6] quit
```

在 Router B 上使能 IPv6 组播路由，在其连接有接收者的接口 GigabitEthernet2/1/1 上使能 MLD，在其它接口上使能 IPv6 PIM-SM，并使能 IPv6 双向 PIM。

```
<RouterB> system-view
[RouterB] ipv6 multicast routing
[RouterB-mrib6] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mld enable
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] ipv6 pim sm
[RouterB-GigabitEthernet2/1/2] quit
[RouterB] interface gigabitethernet 2/1/3
[RouterB-GigabitEthernet2/1/3] ipv6 pim sm
[RouterB-GigabitEthernet2/1/3] quit
[RouterB] ipv6 pim
[RouterB-pim6] bidir-pim enable
[RouterB-pim6] quit
```

在 Router C 上使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-SM，并使能 IPv6 双向 PIM。

```
<RouterC> system-view
[RouterC] ipv6 multicast routing
[RouterC-mrib6] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] ipv6 pim sm
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface gigabitethernet 2/1/2
[RouterC-GigabitEthernet2/1/2] ipv6 pim sm
[RouterC-GigabitEthernet2/1/2] quit
[RouterC] interface loopback 0
[RouterC-LoopBack0] ipv6 pim sm
[RouterC-LoopBack0] quit
[RouterC] ipv6 pim
[RouterC-pim6] bidir-pim enable
```

在 Router D 上使能 IPv6 组播路由，在其连接有接收者的接口 GigabitEthernet2/1/1 上使能 MLD，在其它接口上使能 IPv6 PIM-SM，并使能 IPv6 双向 PIM。

```
<RouterD> system-view
[RouterD] ipv6 multicast routing
[RouterD-mrib6] quit
[RouterD] interface gigabitethernet 2/1/1
[RouterD-GigabitEthernet2/1/1] mld enable
[RouterD-GigabitEthernet2/1/1] quit
[RouterD] interface gigabitethernet 2/1/2
[RouterD-GigabitEthernet2/1/2] ipv6 pim sm
[RouterD-GigabitEthernet2/1/2] quit
[RouterD] interface gigabitethernet 2/1/3
[RouterD-GigabitEthernet2/1/3] ipv6 pim sm
[RouterD-GigabitEthernet2/1/3] quit
[RouterD] ipv6 pim
[RouterD-pim6] bidir-pim enable
[RouterD-pim6] quit
```

(3) 配置 C-BSR 和 C-RP

在 Router C 上将接口 Serial2/1 配置为 C-BSR，并将接口 Loopback0 配置为服务于 IPv6 双向 PIM 的 C-RP。

```
[RouterC-pim6] c-bsr 2002::2
[RouterC-pim6] c-rp 6001::1 bidir
[RouterC-pim6] quit
```

4. 验证配置

通过使用 **display ipv6 pim df-info** 命令可以查看路由器上双向 PIM 的 DF 信息。例如：

显示 Router A 上 IPv6 双向 PIM 的 DF 信息。

```
[RouterA] display ipv6 pim df-info
 RP address: 6001::1
  Interface           State   DF-Pref    DF-Metric  DF-Uptime DF-Address
  GE2/1/1             Win     100        2          01:08:50  FE80::200:5EFF:
                                                              FE71:2800 (local)
  GE2/1/2             Lose    100        1          01:07:49  FE80::20F:E2FF:
                                                              FE38:4E01
```

显示 Router B 上 IPv6 双向 PIM 的 DF 信息。

```
[RouterB] display ipv6 pim df-info
 RP address: 6001::1
  Interface           State   DF-Pref    DF-Metric  DF-Uptime DF-Address
  GE2/1/1             Win     100        1          01:24:09  FE80::200:5EFF:
                                                              FE71:2801 (local)
  GE2/1/2             Win     100        1          01:24:09  FE80::20F:E2FF:
                                                              FE38:4E01 (local)
  GE2/1/3             Lose    0          0          01:23:12  FE80::20F:E2FF:
                                                              FE15:5601
```

显示 Router C 上 IPv6 双向 PIM 的 DF 信息。

```
[RouterC] display ipv6 pim df-info
 RP address: 6001::1
```

```
  Interface           State   DF-Pref    DF-Metric  DF-Uptime DF-Address
  Loop0               -       -          -          -         -
  GE2/1/1             Win     0          0          01:06:07  FE80::20F:E2FF:
                                                               FE15:5601 (local)
  GE2/1/2             Win     0          0          01:06:07  FE80::20F:E2FF:
                                                               FE15:5602 (local)
```

显示 Router D 上 IPv6 双向 PIM 的 DF 信息。

```
[RouterD] display ipv6 pim df-info
 RP address: 6001::1
  Interface           State   DF-Pref    DF-Metric  DF-Uptime DF-Address
  GE2/1/1             Win     100        1          01:19:53  FE80::200:5EFF:
                                                               FE71:2803 (local)
  GE2/1/2             Win     100        1          00:39:34  FE80::200:5EFF:
                                                               FE71:2802 (local)
  GE2/1/3             Lose    0          0          01:21:40  FE80::20F:E2FF:
                                                               FE15:5602
```

通过使用 **display ipv6 multicast forwarding df-info** 命令可以查看路由器上 IPv6 组播转发的 DF 信息，有关 **display ipv6 multicast forwarding df-info** 命令的详细介绍，请参见“IP 组播命令参考”中的“IPv6 组播路由与转发”。例如：

显示 Router A 上 IPv6 组播转发的 DF 信息。

```
[RouterA] display ipv6 multicast forwarding df-info
Total 1 RP, 1 matched

00001. RP address: 6001::1
     Flags: 0x0
     Uptime: 00:08:32
     RPF interface: GigabitEthernet2/1/2
     List of 1 DF interfaces:
       1: GigabitEthernet2/1/1
```

显示 Router B 上 IPv6 组播转发的 DF 信息。

```
[RouterB] display ipv6 multicast forwarding df-info
Total 1 RP, 1 matched

00001. RP address: 6001::1
     Flags: 0x0
     Uptime: 00:06:24
     RPF interface: GigabitEthernet2/1/3
     List of 2 DF interfaces:
       1: GigabitEthernet2/1/1
       2: GigabitEthernet2/1/2
```

显示 Router C 上 IPv6 组播转发的 DF 信息。

```
[RouterC] display ipv6 multicast forwarding df-info
Total 1 RP, 1 matched

00001. RP address: 6001::1
     Flags: 0x0
     Uptime: 00:07:21
```

```
     RPF interface: LoopBack0
     List of 2 DF interfaces:
       1: GigabitEthernet2/1/1
       2: GigabitEthernet2/1/2
```

显示 Router D 上 IPv6 组播转发的 DF 信息。

```
[RouterD] display ipv6 multicast forwarding df-info
Total 1 RP, 1 matched

00001. RP address: 6001::1
     Flags: 0x0
     Uptime: 00:05:12
     RPF interface: GigabitEthernet2/1/3
     List of 2 DF interfaces:
       1: GigabitEthernet2/1/1
       2: GigabitEthernet2/1/2
```

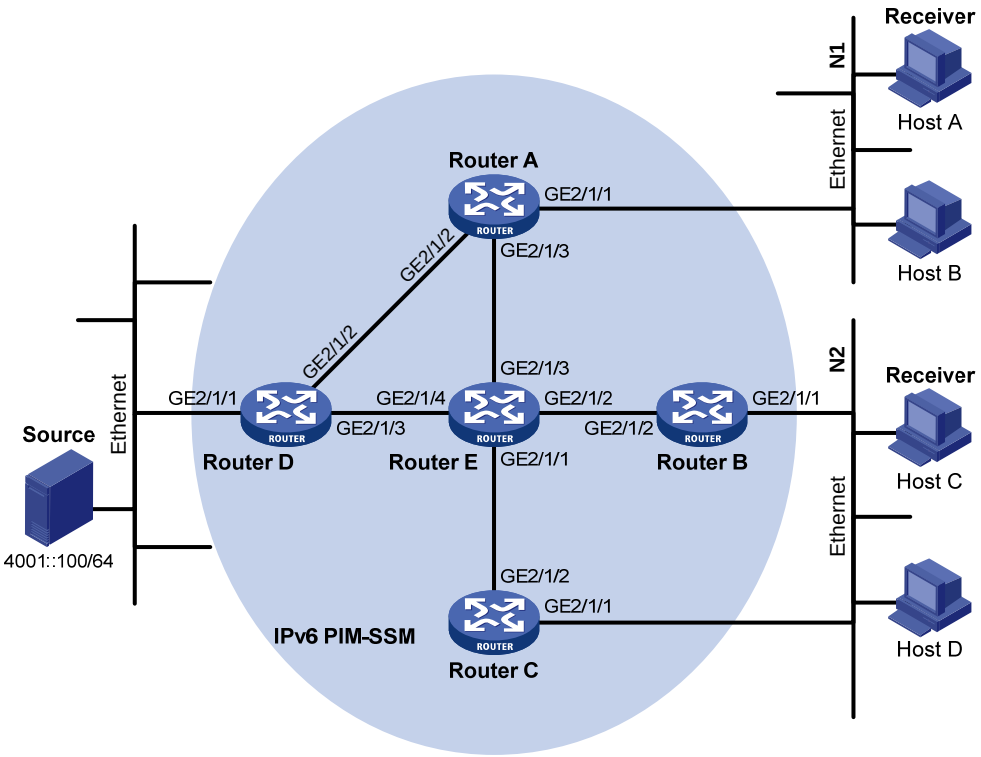
1.8.5 IPv6 PIM-SSM典型配置举例

1. 组网需求

- 接收者通过组播方式接收视频点播信息，不同组织的接收者群体组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 IPv6 PIM 域采用 SSM 方式。
- Host A 和 Host C 为两个末梢网络中的 IPv6 组播信息接收者；Router D 通过 GigabitEthernet2/1/1 接口与 IPv6 组播源（Source）所在网络连接；Router A 通过 GigabitEthernet2/1/1 接口连接末梢网络 N1，通过 GigabitEthernet2/1/2 接口和 GigabitEthernet2/1/3 接口分别连接 Router D 和 Router E；Router B 和 Router C 分别通过各自的 GigabitEthernet2/1/1 接口连接末梢网络 N2，并分别通过各自的 GigabitEthernet2/1/2 接口连接 Router E。
- IPv6 SSM 组播组的范围是 FF3E::/64。
- Router A 与末梢网络 N1 之间运行 MLDv2；Router B 和 Router C 与末梢网络 N2 之间也运行 MLDv2。

2. 组网图

图1-19 IPv6 PIM-SSM 典型配置组网图



设备	接口	IPv6地址	设备	接口	IPv6地址
Router A	GE2/1/1	1001::1/64	Router D	GE2/1/1	4001::1/64
	GE2/1/2	1002::1/64		GE2/1/2	1002::2/64
	GE2/1/3	1003::1/64		GE2/1/3	4002::1/64
Router B	GE2/1/1	2001::1/64	Router E	GE2/1/1	3001::2/64
	GE2/1/2	2002::1/64		GE2/1/2	2002::2/64
Router C	GE2/1/1	2001::2/64		GE2/1/3	1003::2/64
	GE2/1/2	3001::1/64		GE2/1/4	4002::2/64

3. 配置步骤

(1) 配置 IPv6 地址和 IPv6 单播路由协议

请按照 图 1-19 配置各接口的IPv6 地址和前缀长度，具体配置过程略。

配置 IPv6 PIM-SSM 域内的各路由器之间采用 OSPFv3 协议进行互连，确保 IPv6 PIM-SSM 域内部在网络层互通，并且各路由器之间能够借助 IPv6 单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IPv6 组播路由，并使能 IPv6 PIM-SM 和 MLD

在 Router A 上使能 IPv6 组播路由，在其连接末梢网络的接口 GigabitEthernet2/1/1 上使能 MLD，且配置其版本为 2；并在其它接口上使能 IPv6 PIM-SM。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] mld enable
[RouterA-GigabitEthernet2/1/1] mld version 2
```

```
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ipv6 pim sm
[RouterA-GigabitEthernet2/1/2] quit
[RouterA] interface gigabitethernet 2/1/3
[RouterA-GigabitEthernet2/1/3] ipv6 pim sm
[RouterA-GigabitEthernet2/1/3] quit
```

Router B 和 Router C 的配置与 Router A 相似，Router D 和 Router E 除了不需要在相应接口上使能 MLD 外，其它的配置也与 Router A 相似，配置过程略。

(3) 配置 IPv6 SSM 组播组的地址范围

在 Router A 上配置 IPv6 SSM 组播组的地址范围为 FF3E::/64。

```
[RouterA] acl ipv6 number 2000
[RouterA-acl6-basic-2000] rule permit source ff3e:: 64
[RouterA-acl6-basic-2000] quit
[RouterA] ipv6 pim
[RouterA-pim6] ssm-policy 2000
[RouterA-pim6] quit
```

Router B、Router C、Router D 和 Router E 的配置与 Router A 相似，配置过程略。

2. 验证配置

通过使用 **display ipv6 pim interface** 命令可以查看路由器接口上 IPv6 PIM 的配置和运行情况。例如：

显示 Router A 上 IPv6 PIM 的配置信息。

```
[RouterA] display ipv6 pim interface
 Interface             NbrCnt HelloInt   DR-Pri   DR-Address
 GE2/1/1               0      30         1        1001::1
                                                  (local)
 GE2/1/2               1      30         1        1002::2
 GE2/1/3               1      30         1        1003::2
```

假如 Host A 需要接收指定 IPv6 组播源 S（4001::100/64）发往 IPv6 组播组 G（FF3E::101）的信息，Router A 会向 IPv6 组播源方向构造 SPT，SPT 路径中的路由器（Router A 和 Router D）上生成（S，G）表项，而 SPT 路径之外的路由器（Router E）上没有 IPv6 组播路由项，通过使用 **display ipv6 pim routing-table** 命令可以查看路由器的 IPv6 PIM 路由表信息。例如：

显示 Router A 上的 IPv6 PIM 路由表信息。

```
[RouterA] display ipv6 pim routing-table
 Total 0 (*, G) entry; 1 (S, G) entry

 (4001::100, FF3E::101)
     Protocol: pim-ssm, Flag:
     UpTime: 00:00:11
     Upstream interface: GigabitEthernet2/1/2
         Upstream neighbor: 1002::2
         RPF prime neighbor: 1002::2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/1/1
```

```
            Protocol: mld, UpTime: 00:00:11, Expires: 00:03:25
```

显示 Router D 上的 IPv6 PIM 路由表信息。

```
[RouterD] display ipv6 pim routing-table
 Total 0 (*, G) entry; 1 (S, G) entry

 (4001::100, FF3E::101)
     Protocol: pim-ssm, Flag: LOC
     UpTime: 00:08:02
     Upstream interface: GigabitEthernet2/1/1
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/1/2
             Protocol: pim-ssm, UpTime: 00:08:02, Expires: 00:03:25
```

1.9 常见配置错误举例

1.9.1 无法正确建立组播分发树

1. 故障现象

网络中各路由器（包括直连 IPv6 组播源或接收者的路由器）上都没有 IPv6 组播转发项，也就是说无法正确建立组播分发树，客户端无法接收 IPv6 组播数据。

2. 故障分析

- 当全网运行 IPv6 PIM-DM 时，IPv6 组播数据由直连组播源的第一跳路由器扩散到直连客户端的最后一跳路由器。无论 IPv6 组播数据扩散到哪一台路由器，只有该路由器存在到达组播源的路由，才会创建（S，G）表项。反之，如果没有到达组播源的路由或者到达组播源的 RPF 接口没有使能 IPv6 PIM-DM，该路由器就无法创建（S，G）表项。
- 当全网运行 IPv6 PIM-SM 时，路由器在准备加入 SPT 时，只有存在到达组播源的路由，才会创建（S，G）表项。反之，如果没有到达组播源的路由或者到达组播源的 RPF 接口没有使能 IPv6 PIM-SM，该路由器就无法创建（S，G）表项。
- 对于某个 RPF 检查对象，在现存的 IPv6 单播路由表中查找到达该对象的最优路由，该路由的出接口作为 RPF 接口，下一跳作为 RPF 邻居。RPF 接口完全依赖于现存的 IPv6 单播路由，并且与 IPv6 PIM 本身无关。RPF 接口上必须使能 IPv6 PIM，而且 RPF 邻居也必须是 IPv6 PIM 邻居。如果 RPF 接口或 RPF 邻居所在路由器上没有使能 IPv6 PIM，必然使组播分发树无法正确建立，导致 IPv6 组播数据转发异常。
- Hello 报文并不携带 IPv6 PIM 的模式信息，所以运行 IPv6 PIM 的路由器无法掌握自己的 IPv6 PIM 邻居运行的是何种模式的 IPv6 PIM。如果 RPF 接口和 RPF 邻居所在路由器的对应接口没有使能相同模式的 IPv6 PIM，必然使组播分发树无法正确建立，导致 IPv6 组播数据转发异常。
- 全网必须运行相同模式的 IPv6 PIM。否则，组播分发树必然无法正确建立，导致 IPv6 组播数据转发异常。

3. 处理过程

(1) 检查 IPv6 单播路由。使用命令 **display ipv6 routing-table** 命令检查是否有到达 IPv6 组播源或 RP 的 IPv6 单播路由。

(2) 检查接口上是否使能了 IPv6 PIM，尤其是 RPF 接口上是否使能了 IPv6 PIM。通过命令 **display ipv6 pim interface** 命令查看接口上的 IPv6 PIM 信息。若接口上未使能 IPv6 PIM，请使用 **ipv6 pim dm** 或 **ipv6 pim sm** 命令使能 IPv6 PIM-DM 或 IPv6 PIM-SM。

(3) 检查 RPF 邻居是否是 IPv6 PIM 邻居。通过 **display ipv6 pim neighbor** 命令查看 IPv6 PIM 邻居的信息。

(4) 检查直连 IPv6 组播源或接收者的路由器接口上是否使能了 IPv6 PIM 和 MLD。

(5) 检查 IPv6 PIM 模式是否一致。通过命令 **display ipv6 pim interface verbose** 检查 RPF 接口和 RPF 邻居所在路由器的对应接口上是否使能了相同模式的 IPv6 PIM。

(6) 检查全网各路由器上的 IPv6 PIM 模式是否一致。通过命令 **display current-configuration** 查看接口上的 IPv6 PIM 模式信息，确保全网所有路由器配置有相同模式的 IPv6 PIM。如果都配置为 IPv6 PIM-SM，则还需检查 BSR 以及 C-RP 的配置是否正确。

1.9.2 IPv6 组播数据异常终止在中间路由器

1. 故障现象

IPv6 组播数据可以到达中间路由器，但无法到达最后一跳路由器。中间路由器某接口上收到 IPv6 组播数据，但 IPv6 PIM 路由表中没有创建相应的（S，G）表项。

2. 故障分析

- 命令 **ipv6 multicast boundary** 用于在接口上设置 IPv6 组播转发边界，如果 IPv6 组播数据无法通过该边界，IPv6 PIM 将无法创建路由项。
- 此外，**source-policy** 命令用于过滤接收到的 IPv6 组播数据报文。如果 IPv6 组播数据报文无法通过该命令中的 ACL 规则，IPv6 PIM 也无法创建路由项。

3. 处理过程

(1) 检查 IPv6 组播转发边界的配置。通过命令 **display current-configuration** 查看 IPv6 组播转发边界上的设置，使用 **ipv6 multicast boundary** 命令更改 IPv6 组播转发边界的设置，使 IPv6 组播数据能够通过该边界。

(2) 检查 IPv6 组播过滤器配置。通过命令 **display current-configuration** 查看 IPv6 组播过滤器的配置，更改 **source-policy** 命令的 ACL 规则，使 IPv6 组播数据的源/组地址通过 ACL 过滤。

1.9.3 IPv6 PIM-SM中RP无法加入SPT

1. 故障现象

RPT 无法正确建立，或者 RP 无法加入到达 IPv6 组播源的 SPT。

2. 故障分析

- RP 是 IPv6 PIM-SM 网络的核心，为特定的 IPv6 组播组服务，网络中可以同时存在多个 RP。必须保证所有路由器上的 RP 信息完全一致，并且相同的 IPv6 组播组映射到相同的 RP，否则将导致 IPv6 组播数据转发异常。

- 如果使用了静态 RP，必须在全网所有路由器上配置完全相同的静态 RP，否则将导致 IPv6 组播数据转发异常。

3. 处理过程

(1) 检查是否有到达 RP 的 IPv6 单播路由。通过命令 **display ipv6 routing-table** 查看各路由器上是否有到达 RP 的 IPv6 单播路由。

(2) 检查动态 RP 的信息。通过命令 **display ipv6 pim rp-info** 查看各路由器上的 RP 信息是否一致。

(3) 检查静态 RP 的配置。通过命令 **display ipv6 pim rp-info** 查看全网所有路由器上的静态 RP 配置是否完全相同。

1.9.4 IPv6 PIM-SM中无法建立RPT或无法进行源注册

1. 故障现象

C-RP 无法向 BSR 单播通告报文，BSR 没有发布包含 C-RP 的自举报文，BSR 上没有到达各 C-RP 的 IPv6 单播路由，RPT 无法正确建立，或者 DR 无法向 RP 进行源注册。

2. 故障分析

- C-RP 周期性地向 BSR 单播宣告报文，如果 C-RP 没有到达 BSR 的 IPv6 单播路由就无法发送宣告报文，BSR 就收不到 C-RP 宣告报文，也就不会发布包含该 C-RP 的自举报文。
- 另外，如果 BSR 没有到达 C-RP 的 IPv6 单播路由，就会丢弃 C-RP 发来的宣告报文，也不会发布包含该 C-RP 的自举报文。
- RP 是 IPv6 PIM-SM 网络的核心。必须保证全网所有路由器的 RP 信息完全一致，并且特定的组 G 映射到相同的 RP，以及存在到达 RP 的 IPv6 单播路由。

3. 处理过程

(1) 检查是否有到各 C-RP、BSR 的 IPv6 单播路由。通过命令 **display ipv6 routing-table** 查看各路由器上是否有到达 C-RP 和 BSR 的路由，以及 C-RP 和 BSR 之间的路由是否可达。确保各 C-RP 上存在到达 BSR 的路由，BSR 上存在到达各 C-RP 的路由，全网所有路由器上存在到达 C-RP 的路由。

(2) 检查 RP 和 BSR 信息。IPv6 PIM-SM 协议需要有 RP 和 BSR 的支持，首先使用命令 **display ipv6 pim bsr-info** 查看各路由器上是否有 BSR 的信息，使用 **display ipv6 pim rp-info** 命令查看各路由器上的 RP 信息是否正确。

(3) 检查 IPv6 PIM 邻居关系。通过命令 **display ipv6 pim neighbor** 查看各路由器之间是否正确建立了邻居关系。