# 4 PIM（IPv4）配置

## 关于本章

通过配置PIM（IPv4）协议，可以实现组播数据在IPv4网络的组播路由与转发。

4.1 PIM协议简介
介绍PIM协议的定义和目的。

4.2 PIM原理描述
介绍PIM协议的实现原理。

4.3 PIM应用场景
介绍组播PIM协议的应用场景。

4.4 配置PIM（IPv4）任务概览
PIM协议配置完成后，就可实现组播数据在IPv4网络的组播路由与转发。PIM协议包含多种不同类型的模式，不同模式的PIM协议适用于不同的应用场景。

4.5 PIM（IPv4）配置注意事项
介绍配置PIM（IPv4）的注意事项。

4.6 PIM（IPv4）缺省配置
介绍缺省情况下，PIM的配置信息。

4.7 配置PIM-DM（IPv4）
通过配置PIM-DM协议，可以实现域内组播路由与数据转发。PIM-DM是密集模式的域内组播路由协议，适用于组成员分布相对集中、范围较小的网络。

4.8 配置PIM-SM（IPv4）
通过配置PIM协议，可以实现域内组播路由与数据转发。PIM-SM是稀疏模式的域内组播路由协议，适用于组成员分布相对分散、范围较广的大规模网络。

4.9 维护PIM-DM
PIM-DM的维护包括：清除PIM控制报文统计信息、监控PIM的运行状况。

4.10 维护PIM-SM
PIM-SM的维护包括：清除PIM控制报文统计信息、清除PIM路由表项下游接口的状态、监控PIM的运行状况。

4.11 PIM（IPv4）配置举例
介绍PIM（IPv4）协议常用功能的配置示例。

# 4.1 PIM 协议简介

介绍PIM协议的定义和目的。

## 定义

PIM（Protocol Independent Multicast）称为协议无关组播。这里的协议无关指的是与单播路由协议无关，即PIM不需要维护专门的单播路由信息。作为组播路由解决方案，它直接利用单播路由表的路由信息，对组播报文执行RPF（Reverse Path Forwarding，逆向路径转发）检查，检查通过后创建组播路由表项，从而转发组播报文。

目前设备实际支持的PIM协议包括：PIM-DM（PIM-Dense Mode）、PIM-SM（PIM-Sparse Mode）。

## 目的

1992年，为了承载网络视频会议、音频会议，以MOSPF和DVMRP为组播路由协议的虚拟IP组播骨干网——Mbone建立成功。这为组播技术应用和推广起到了积极作用，在随后的十几年，组播路由协议得到了很大发展。

但是随着多个组播路由协议的开发与应用，人们渐渐感觉到，如果像单播路由一样通过多种路由协议算法来动态生成组播路由，会带来不同路由协议间在互相引入路由时操作繁琐的问题。而且网络设备对于单播和组播路由信息都需要维护。这也就催生了一种与单播路由协议无关的组播路由协议——PIM。PIM协议只专注于组成员和组播源状态相关的信息，而选取路径的信息直接从单播路由表获取。因此它不需要维护庞大的路由信息，从而降低了PIM协议的复杂性。这使得PIM协议成为应用最广泛的域内组播协议。

**说明**

由PIM路由器所组成的网络称为PIM网络。通常一个大的PIM网络可以划分为多个PIM域来管理和控制组播报文的转发，这里的域内组播协议即是指PIM域内组播协议。

# 4.2 PIM 原理描述

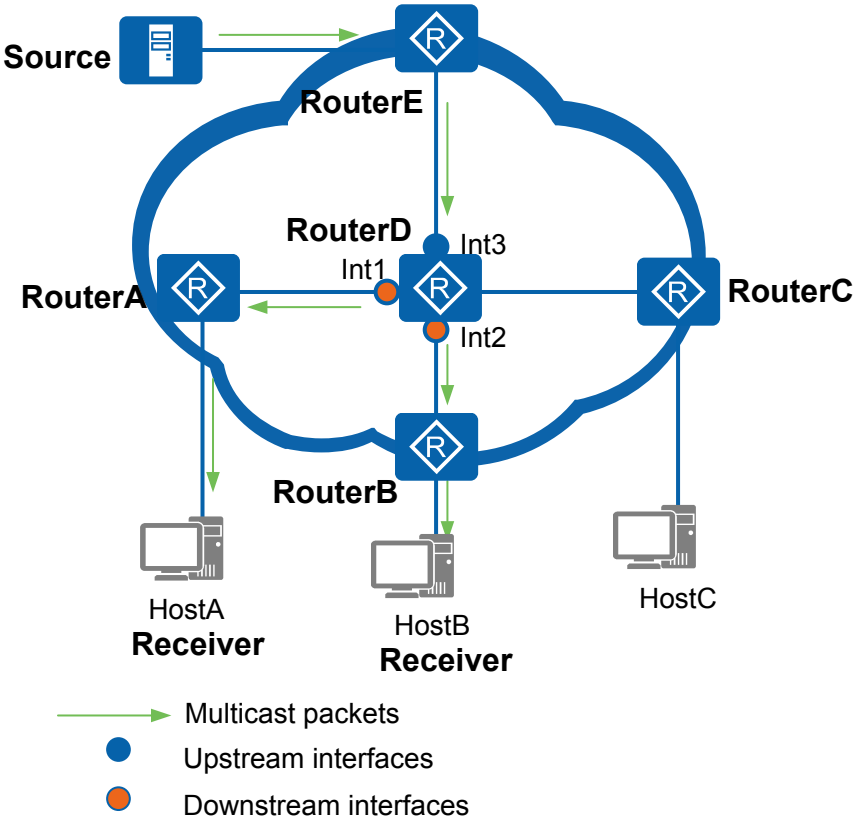
介绍PIM协议的实现原理。

## 4.2.1 基本概念

通过**图1**来介绍PIM的一些基本概念。

**图 4-1** PIM 网络示意图




## 组播分发树

PIM网络以组播组为单位在路由器上建立一点到多点的组播转发路径。由于组播转发路径呈现树型结构，也称为组播分发树MDT（Multicast Distribution Tree）。

组播分发树主要包括以下两种：

- 以组播源为根，组播组成员为叶子的组播分发树称为SPT（Shortest Path Tree）。SPT同时适用于PIM-DM网络和PIM-SM网络。

  如图1中的RouterE→RouterD→RouterA（RouterB），就是一棵以Source为根，以HostA、HostB为叶子的SPT。
- 以RP（Rendezvous Point）为根，组播组成员为叶子的组播分发树称为RPT（RP Tree）。RPT适用于PIM-SM网络。

  有关RP以及RPT的详细介绍请参见**4.2.3 PIM-SM（ASM模型）**。

## PIM 路由器

在接口上使能了PIM协议的路由器即为PIM路由器。在建立组播分发树的过程中，PIM路由器又分为以下几种：

- 叶子路由器：与用户主机相连的PIM路由器，但连接的用户主机不一定为组成员，如图1中的RouterA、RouterB、RouterC。
- 第一跳路由器：组播转发路径上，与组播源相连且负责转发该组播源发出的组播数据的PIM路由器。如图1中的RouterE。
- 最后一跳路由器：组播转发路径上，与组播组成员相连且负责向该组成员转发组播数据的PIM路由器。如图1中的RouterA、RouterB。

- 中间路由器：组播转发路径上，第一跳路由器与最后一跳路由器之间的PIM路由器。如图1中的RouterD。

### PIM 路由表项

PIM路由表项即通过PIM协议建立的组播路由表项。PIM网络中存在两种路由表项：（S，G）路由表项或（*，G）路由表项。S表示组播源，G表示组播组，*表示任意。

- （S，G）路由表项主要用于在PIM网络中建立SPT。对于PIM-DM网络和PIM-SM网络适用。
- （*，G）路由表项主要用于在PIM网络中建立RPT。对于PIM-SM网络适用。

PIM路由器上可能同时存在两种路由表项。当收到源地址为S，组地址为G的组播报文，且RPF检查通过的情况下，按照如下的规则转发：

- 如果存在（S，G）路由表项，则由（S，G）路由表项指导报文转发。
- 如果不存在（S，G）路由表项，只存在（*，G）路由表项，则先依照（*，G）路由表项创建（S，G）路由表项，再由（S，G）路由表项指导报文转发。

PIM路由表项中主要用于指导转发的信息如下：

- 组播源地址。
- 组播组地址。
- 上游接口：本地路由器上接收到组播数据的接口，如图1中的Int3。
- 下游接口：将组播数据转发出去的接口，如图1中的Int1、Int2。

## 4.2.2 PIM-DM

### 基本原理

PIM-DM使用“推（Push）模式”转发组播报文，一般应用于组播组成员规模相对较小、相对密集的网络。在实现过程中，它会假设网络中的组成员分布非常稠密，每个网段都可能存在组成员。当有活跃的组播源出现时，PIM-DM会将组播源发来的组播报文扩散到整个网络的PIM路由器上，再裁剪掉不存在组成员的分支。PIM-DM通过周期性的进行“扩散（Flooding）—剪枝（Prune）”，来构建并维护一棵连接组播源和组成员的单向无环SPT（Source Specific Shortest Path Tree）。如果在下一次“扩散-剪枝”进行前，被裁剪掉的分支由于其叶子路由器上有新的组成员加入而希望提前恢复转发状态，也可通过嫁接（Graft）机制主动恢复其对组播报文的转发。

PIM-DM的关键工作机制包括邻居发现、扩散、剪枝、嫁接、断言和状态刷新。其中，扩散、剪枝、嫁接是构建SPT的主要方法。

### 邻居发现（Neighbor Discovery）

PIM路由器上每个使能了PIM协议的接口都会对外发送Hello报文。封装Hello报文的组播报文的目的地址是224.0.0.13（表示同一网段中所有PIM路由器）、源地址为接口的IP地址、TTL数值为1。

Hello报文的作用：发现PIM邻居、协调各项PIM协议报文参数、维持邻居关系。

- 发现PIM邻居

同一网段中的PIM路由器都必须接收目的地址为224.0.0.13的组播报文。这样直接相连的PIM路由器之间通过交互Hello报文以后，就可以彼此知道自己的邻居信息，建立邻居关系。

只有邻居关系建立成功后，PIM路由器才能接收其他PIM协议报文，从而创建组播路由表项。

- 协调各项PIM协议报文参数

  Hello报文中携带多项PIM协议报文参数，主要用于PIM邻居之间PIM协议报文的控制。具体如下：

  - DR_Priority：表示各路由器接口竞选DR的优先级，优先级越高越容易获胜。
  - Holdtime：表示保持邻居为可达状态的超时时间。如果在超时时间内没有收到PIM邻居发送的Hello报文，路由器则认为邻居不可达。
  - LAN_Delay：表示共享网段内传输Prune报文的延迟时间。
  - Neighbor-Tracking：表示邻居跟踪功能。
  - Override-Interval：表示Hello报文中携带的否决剪枝的时间间隔。

  **说明**

  参数DR_Priority只在PIM-SM网络的DR竞选中用到。有关DR竞选的内容请参见**“PIM-SM（ASM模型）DR竞选”**。

- 维持邻居关系

  PIM路由器之间周期性地发送Hello报文。如果Holdtime超时还没有收到该PIM邻居发出的新的Hello报文，PIM路由器就认为该邻居不可达，将其从邻居列表中清除。

  PIM邻居的变化将导致网络中组播拓扑的变化。如果组播分发树上的某上游邻居或下游邻居不可达，将导致组播路由重新收敛，组播分发树迁移。

## 扩散（Flooding）

当PIM-DM网络中出现活跃的组播源之后，组播源发送的组播报文将在全网内扩散。当PIM路由器接收到组播报文，根据单播路由表进行RPF检查通过后，就会在该路由器上创建（S，G）表项，下游接口列表中包括除上游接口之外与所有PIM邻居相连的接口，后续到达的组播报文将从各个下游接口转发出去。

最后组播报文扩散到达叶子路由器，会出现以下两种情况：

- 若与该叶子路由器相连用户网段上存在组成员，则将与该网段相连的接口加入（S，G）表项的下游接口列表中，后续的组播报文会向组成员转发。
- 若与该叶子路由器相连用户网段上不存在组成员，且不需要向其下游PIM邻居转发组播报文，则执行**剪枝**动作。

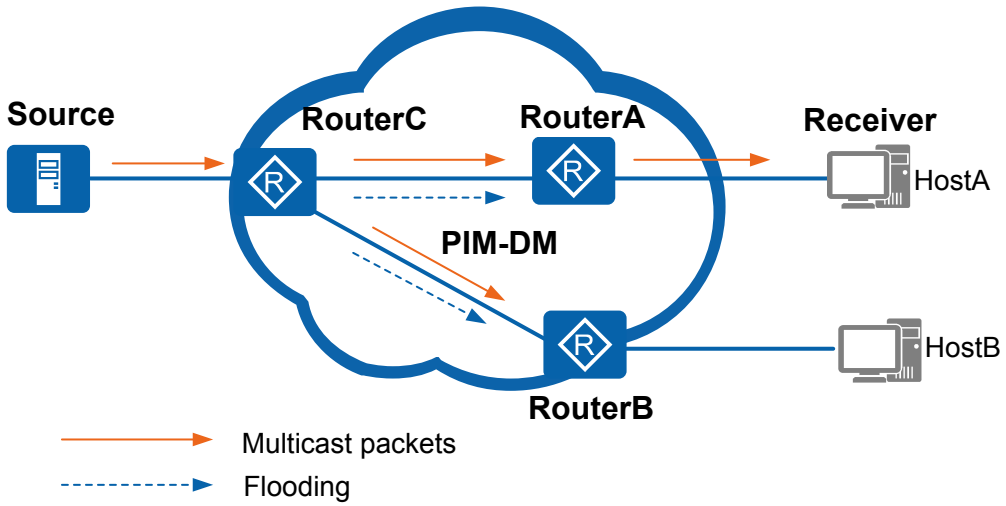
**说明**

有时组播报文扩散到一个连着多台PIM路由器的共享网段时，会出现这种情况：这些PIM路由器上进行的RPF检查都能通过，从而有多份相同报文转发到这个网段。此时，需要执行**断言**动作。

如**图1**所示，在PIM-DM网络中，RouterA、RouterB和RouterC之间通过发送Hello报文建立了PIM邻居关系。HostA通过RouterA与HostA之间运行的IGMP协议加入了组播组G，HostB没有加入任何组播组。

**图 4-2** 扩散示意图




扩散过程如下：

1. 组播源S开始向组播组G发送组播报文。
2. RouterC接收到源发送的组播报文后，根据单播路由表进行RPF检查。RPF检查通过，创建（S，G）表项，下游接口列表包括与RouterA和RouterB相连的接口，后续到达的报文向RouterA和RouterB转发。
3. RouterA接收到来自RouterC的组播报文，RPF检查成功，在本地创建对应（S，G）表项，下游接口列表添加与组成员HostA相连的接口，后续到达的报文向HostA转发。
4. RouterB接收到来自RouterC的组播报文，由于与RouterB相连下游网段不存在组成员和PIM邻居，执行剪枝。

## 剪枝（Prune）

当PIM路由器接收到组播报文后，RPF检查通过，但是下游网段没有组播报文需求。此时PIM路由器会向上游发送剪枝报文，通知上游路由器禁止相应下游接口的转发，将其从（S，G）表项的下游接口列表中删除。剪枝操作由叶子路由器发起，逐跳向上，最终组播转发路径上只存在与组成员相连的分支。

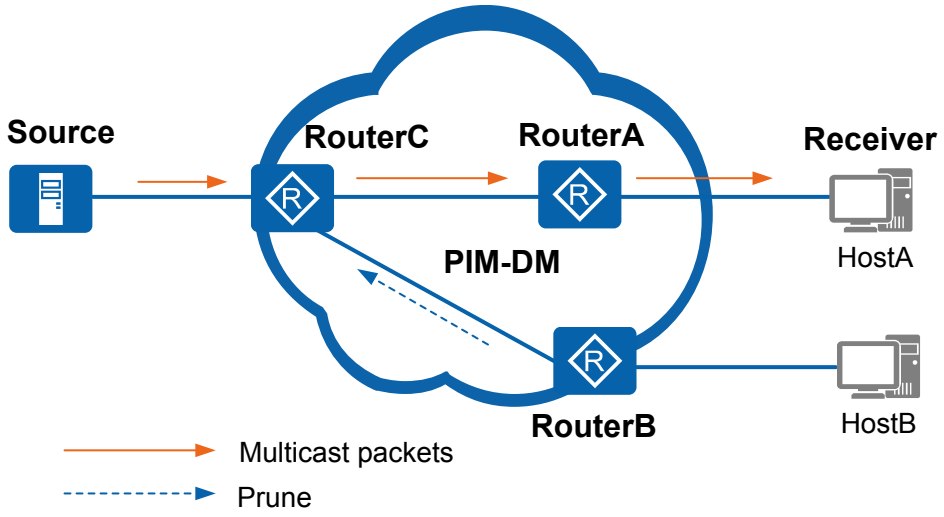
路由器为被裁剪的下游接口启动一个剪枝定时器，定时器超时后接口恢复转发。组播报文重新在全网范围内扩散，新加入的组成员可以接收到组播报文。随后，下游不存在组成员的叶子路由器将向上发起剪枝操作。通过这种周期性的扩散-剪枝，PIM-DM周期性的刷新SPT。

当下游接口被剪枝后：

- 如果下游叶子路由器有组成员加入，并且希望在下次“扩散-剪枝”前就恢复组播报文转发，则执行**嫁接**动作。
- 如果下游叶子路由器一直没有组成员加入，希望该接口保持抑制转发状态，则执行**状态刷新**动作。

如**图2**所示，RouterB上未连接组成员，这种情况下，RouterB向上游发起剪枝。

**图 4-3** 剪枝示意图




剪枝过程如下：

1. RouterB向上游RouterC发送Prune报文，通知RouterC不用再转发数据到该下游网段。
2. RouterC收到Prune报文后，停止该下游接口转发，将该下游接口从（S，G）表项中删除。由于RouterC上还存在其他处于转发状态的下游接口，剪枝过程停止。后续到达的报文只向RouterA转发。

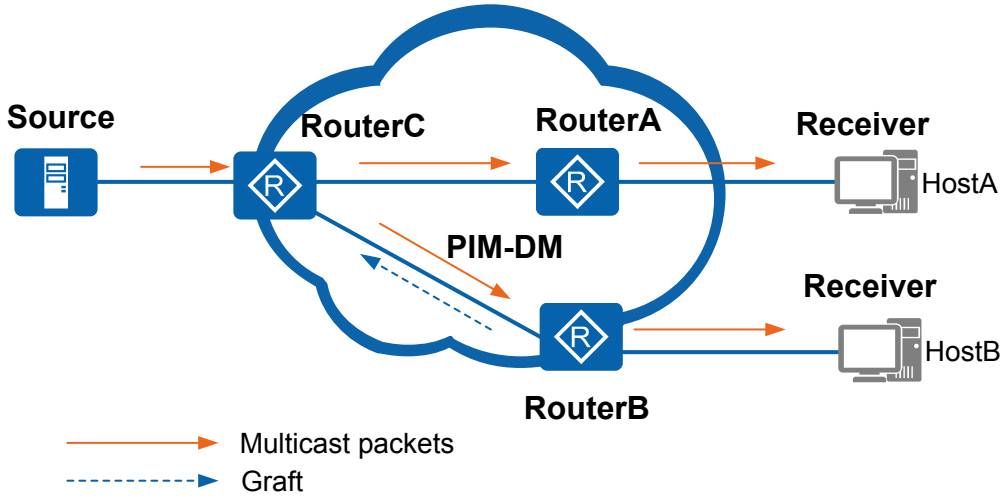
## 嫁接（Graft）

PIM-DM通过嫁接机制，使有新组成员加入的网段快速得到组播报文。叶子路由器通过IGMP了解到与其相连的用户网段上，组播组G有新的组成员加入。随后叶子路由器会向上游发送Graft报文，请求上游路由器恢复相应出接口转发，将其添加在（S，G）表项下游接口列表中。

嫁接过程从叶子路由器开始，到有组播报文到达的路由器结束。

剪枝过程结束后，在下一次“扩散-剪枝”来临前，RouterC不再对下游路由器RouterB转发组播报文。这时，HostB加入组播组G，RouterB向上游发起嫁接，如图3所示。

**图 4-4** 嫁接示意图



嫁接过程如下：

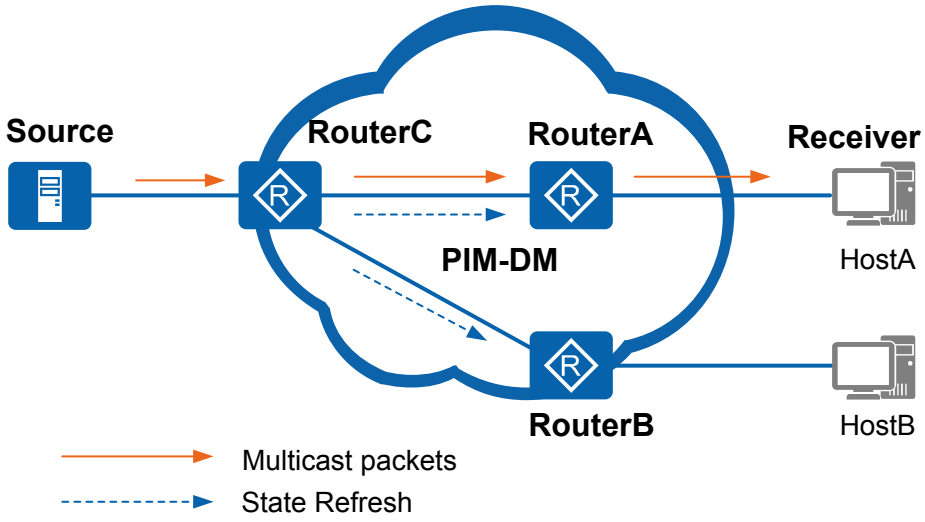
1. RouterB希望在下一次“扩散-剪枝”来临前恢复对HostB组播报文的转发，向上游路由器RouterC发送Graft报文，请求恢复相应出接口转发组播报文。
2. RouterC收到Graft报文后，恢复该接口转发，将该接口添加到（S，G）表项中的下游接口列表中。由于RouterC上有组播报文到达，嫁接过程停止。后续到达的报文向RouterB转发。

## 状态刷新（State Refresh）

在PIM-DM网络中，为了避免被裁剪的接口因为“剪枝定时器”超时而恢复转发，离组播源最近的第一跳路由器会周期性地触发State Refresh报文在全网内扩散。收到State Refresh报文的PIM路由器会刷新剪枝定时器的状态。被裁剪接口的下游叶子路由器如果一直没有组成员加入，该接口将一直处于抑制转发状态。

如图4所示，与RouterC上被裁剪接口相连的叶子路由器上一直没有组成员加入。

**图 4-5 状态刷新示意图**




状态刷新过程如下：

1. RouterC触发状态刷新，将State Refresh报文向RouterA和RouterB扩散。
2. RouterC上存在被裁剪接口，刷新该接口的“剪枝定时器”的状态。下一次“扩散-剪枝”来临时，由于RouterB上仍然没有组成员加入，RouterC上被裁剪的接口将被抑制转发组播报文。

## 断言（Assert）

当一个网段内有多个相连的PIM路由器RPF检查通过向该网段转发组播报文时，则需要通过断言机制来保证只有一个PIM路由器向该网段转发组播报文。PIM路由器在接收到邻居路由器发送的相同组播报文后，会以组播的方式向本网段的所有PIM路由器发送Assert报文，其中目的地址为永久组地址224.0.0.13。其它PIM路由器在接收到Assert报文后，将自身参数与对方报文中携带的参数做比较，进行Assert竞选。竞选规则如下：

1. 单播路由协议优先级较高者获胜。
2. 如果优先级相同，则到组播源的开销较小者获胜。

3. 如果以上都相同，则下游接口IP地址最大者获胜。

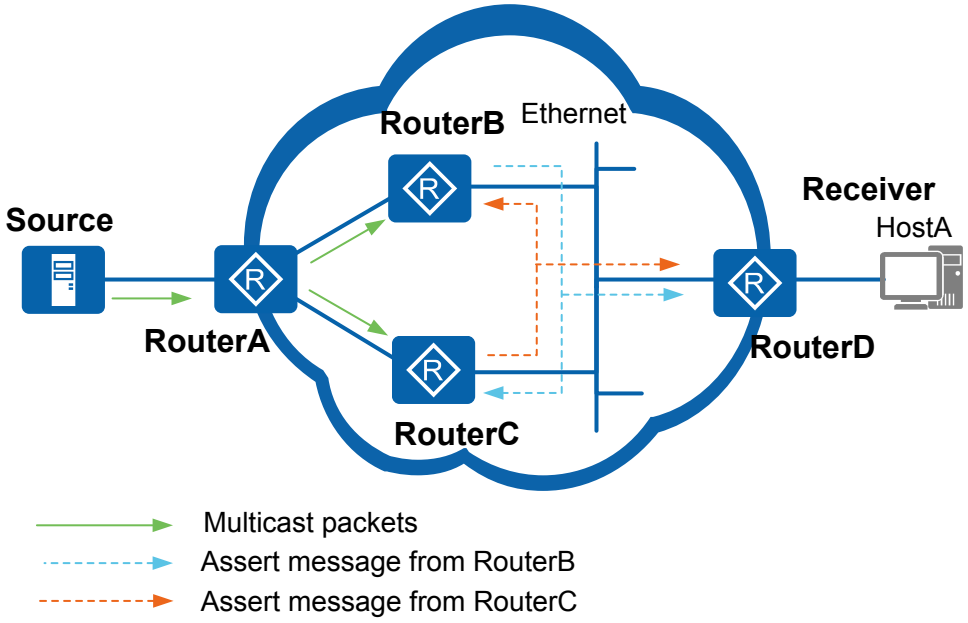
根据Assert竞选结果，路由器将执行不同的操作：

- 获胜一方的下游接口称为Assert Winner，将负责后续对该网段组播报文的转发。
- 落败一方的下游接口称为Assert Loser，后续不会对该网段转发组播报文，PIM路由器也会将其从（S，G）表项下游接口列表中删除。

Assert竞选结束后，该网段上只存在一个下游接口，只传输一份组播报文。所有Assert Loser可以周期性地恢复组播报文转发，从而引发周期性的Assert竞选。

如图5所示，RouterB和RouterC均通过了RPF检查，创建了（S，G）表项。并且两者的下游接口连接在同一网段，RouterB和RouterC都向该网段发送组播报文。

**图 4-6 断言示意图**




断言过程如下：

1. RouterB和RouterC从各自下游接口接收到对方发来的组播报文，RPF检查都失败，报文被丢弃。同时，RouterB和RouterC分别向该网段发送Assert报文。
2. RouterB将自身的路由信息与RouterC发来的Assert报文中携带的路由信息进行比较，由于自身到组播源的开销较小而获胜。于是后续组播报文仍然向该网段转发，RouterC在接收到组播报文后仍然由于RPF检查失败而丢弃。
3. RouterC将自身的路由信息与RouterB发来的Assert报文中携带的路由信息进行比较，由于自身到组播源的开销较大而落败。于是禁止相应下游接口向该网段转发组播报文，将其从（S，G）表项的下游接口列表中删除。

## 4.2.3 PIM-SM（ASM 模型）

### 基本原理

在ASM（Any-Source Multicast）模型中，PIM-SM使用“拉（Pull）模式”转发组播报文，一般应用于组播组成员规模相对较大、相对稀疏的网络。基于这一种稀疏的网络模型，它的实现方法是：

- 在网络中维护一台重要的PIM路由器：汇聚点RP（Rendezvous Point），可以为随时出现的组成员或组播源服务。网络中所有PIM路由器都知道RP的位置。
- 当网络中出现组成员（用户主机通过IGMP加入某组播组G）时，最后一跳路由器向RP发送Join报文，逐跳创建（*，G）表项，生成一棵以RP为根的RPT。
- 当网络中出现活跃的组播源（组播源向某组播组G发送第一个组播数据）时，第一跳路由器将组播数据封装在Register报文中单播发往RP，在RP上创建（S，G）表项，注册源信息。

在ASM模型中，PIM-SM的关键机制包括邻居发现、DR竞选、RP发现、RPT构建、组播源注册、SPT切换、断言；同时也可通过配置BSR（Bootstrap Router）管理域来实现单个PIM-SM域的精细化管理。

## 邻居发现

邻居发现机制与PIM-DM中的相同，详细内容请参见**“PIM-DM邻居发现”**。

## DR 竞选

在组播源或组成员所在的网段，通常同时连接着多台PIM路由器。这些PIM路由器之间通过交互Hello报文成为PIM邻居，Hello报文中携带DR优先级和该网段接口地址。PIM路由器将自身条件与对方报文中携带的信息进行比较，选举出DR来负责源端或组成员端组播报文的收发。竞选规则如下：

- DR优先级较高者获胜（网段中所有PIM路由器都支持DR优先级）。
- 如果DR优先级相同或该网段存在至少一台PIM路由器不支持在Hello报文中携带DR优先级，则IP地址较大者获胜。

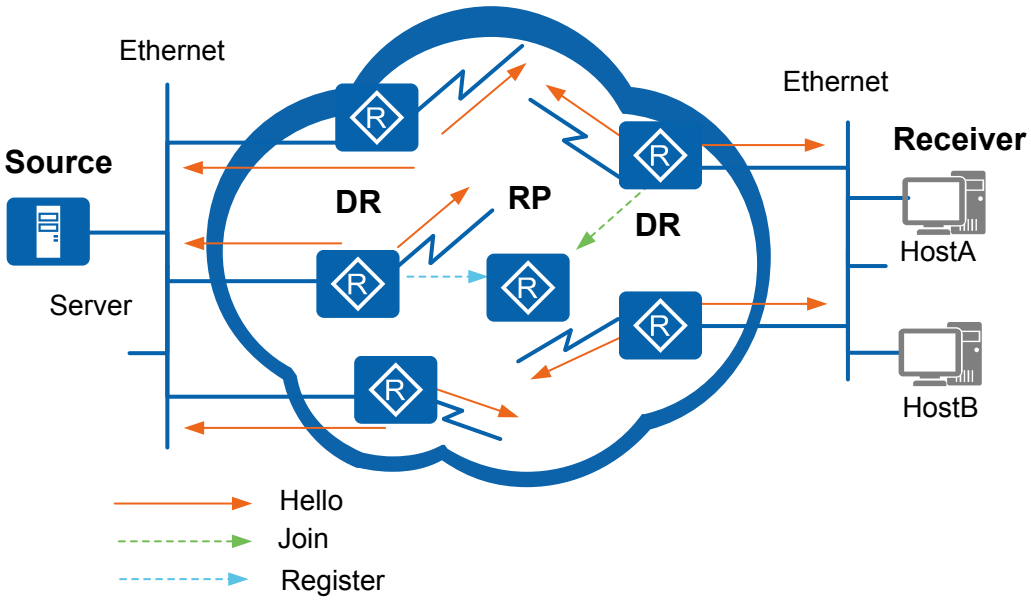
如果当前DR出现故障，将导致PIM邻居关系超时，其他PIM邻居之间会触发新一轮的DR竞选。

如**图4-7**所示，在ASM模型中，DR主要作用如下：

- 在连接组播源的共享网段，由DR负责向RP发送Register注册报文。与组播源相连的DR称为源端DR。
- 在连接组成员的共享网段，由DR负责向RP发送Join加入报文。与组成员相连的DR称为组成员端DR。

**图 4-7** DR 竞选示意图




## RP 发现

汇聚点RP为网络中一台重要的PIM路由器，用于处理源端DR注册信息及组成员加入请求，网络中的所有PIM路由器都必须知道RP的地址，类似于一个供求信息的汇聚中心。

一个RP可以同时为多个组播组服务，但一个组播组只能对应一个RP。目前可以通过以下方式配置RP：

- 静态RP：在网络中的所有PIM路由器上配置相同的RP地址，静态指定RP的位置。
- 动态RP：在PIM域内选择几台PIM路由器，配置C-RP（Candidate-RP，候选RP）来动态竞选出RP。同时，还需要通过配置C-BSR（Candidate-BSR，候选BSR）选举出BSR，来收集C-RP的通告信息，向PIM-SM域内的所有PIM路由器发布。

  C-BSR在竞选的时候，开始时每个C-BSR都认为自己是BSR，向全网发送Bootstrap报文。Bootstrap报文中携带C-BSR地址、C-BSR的优先级。每一台PIM路由器都收到所有C-BSR发出的Bootstrap报文，通过比较这些C-BSR信息，竞选产生BSR。竞选规则如下：

  - 优先级较高者获胜（优先级数值越大优先级越高）。
  - 如果优先级相同，IP地址较大者获胜。

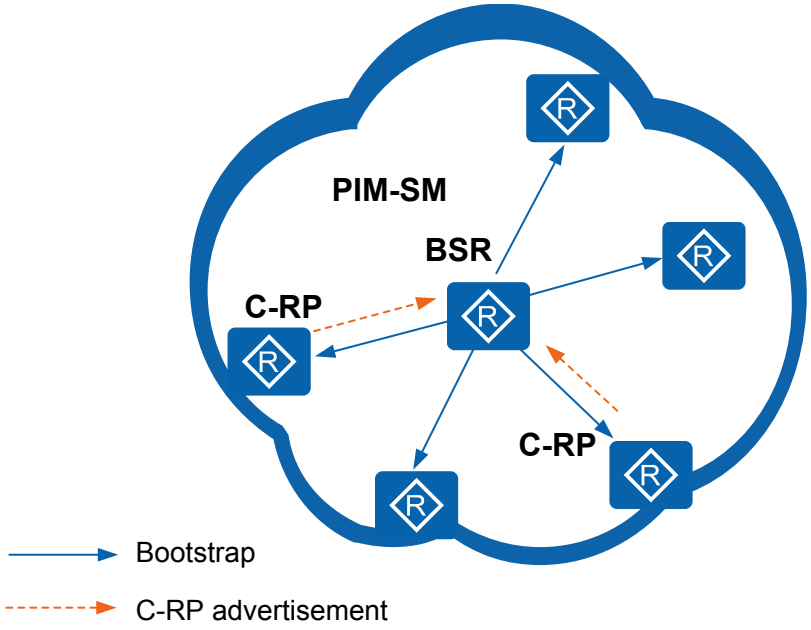
  C-RP的竞选过程如图4-8所示。

  a. C-RP向BSR发送Advertisement报文，报文中携带C-RP地址、服务的组范围和C-RP优先级。
  b. BSR将这些信息汇总为RP-Set，封装在Bootstrap报文中，发布给全网的每一台PIM-SM路由器。
  c. 各PIM路由器根据RP-Set，使用相同的规则进行计算和比较，从多个针对特定组的C-RP中竞选出该组RP。规则如下：
     - 与用户加入的组地址匹配的C-RP服务的组范围掩码最长者获胜。
     - 如果以上比较结果相同，则C-RP优先级较高者获胜（优先级数值越小优先级越高）。
     - 如果以上比较结果都相同，则执行Hash函数，计算结果较大者获胜。

- 如果以上比较结果都相同，则C-RP的IP地址较大者获胜。

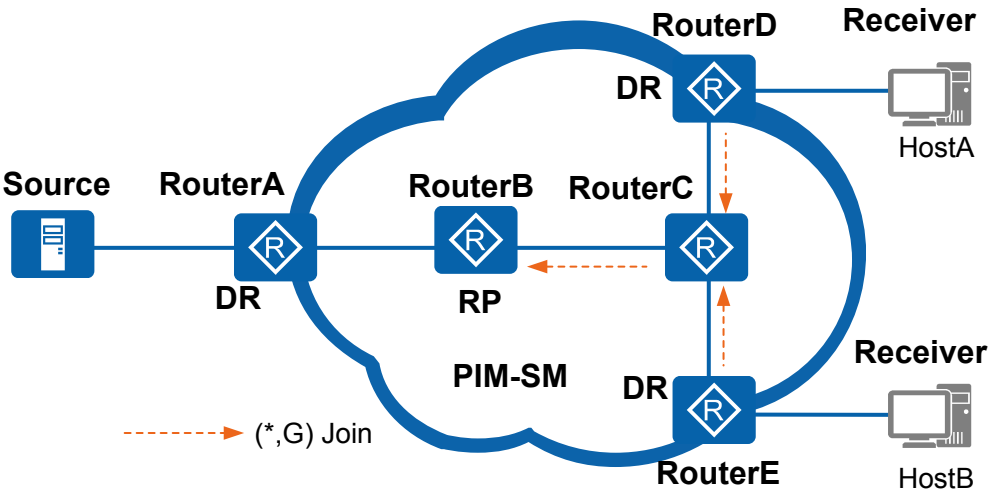
d. 由于所有PIM路由器使用相同的RP-Set和竞选规则，所以得到的组播组与RP之间的对应关系也相同。PIM路由器将“组播组—RP”对应关系保存下来，指导后续的组播操作。

**图 4-8** 动态 RP 竞选机制示意图




## RPT 构建

**图 4-9** RPT 构建示意图

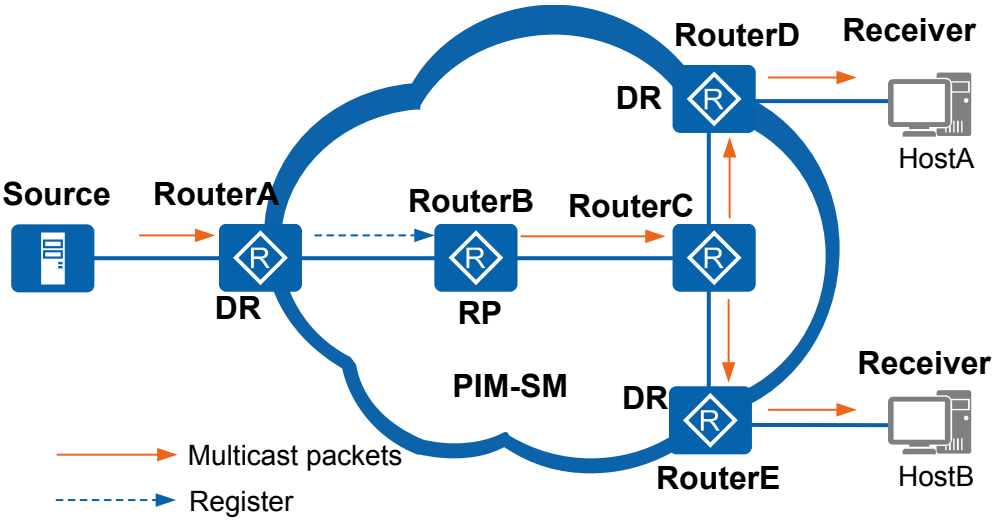



PIM-SM RPT是一棵以RP为根，以存在组成员关系的PIM路由器为叶子的组播分发树。如图4-9所示，当网络中出现组成员（用户主机通过IGMP加入某组播组G）时，组成员端DR向RP发送Join报文，在通向RP的路径上逐跳创建（*，G）表项，生成一棵以RP为根的RPT。

在RPT构建过程中，PIM路由器在发送Join报文时，会进行**RPF检查**：查找到达RP的单播路由，单播路由的出接口为上游接口，下一跳为RPF邻居。Join报文从组成员端DR开始逐跳发送，直至到RP。

## 组播源注册

**图 4-10** 组播源注册示意图




如**图4-10**所示，在PIM-SM网络中，任何一个新出现的组播源都必须首先在RP处“注册”，继而才能将组播报文传输到组成员。具体过程如下：

1. 组播源将组播报文发给源端DR。
2. 源端DR接收到组播报文后，将其封装在Register报文中，发送给RP。
3. RP接收到Register报文，将其解封装，建立（S，G）表项，并将组播数据沿RPT发送到达组成员。

## SPT 切换

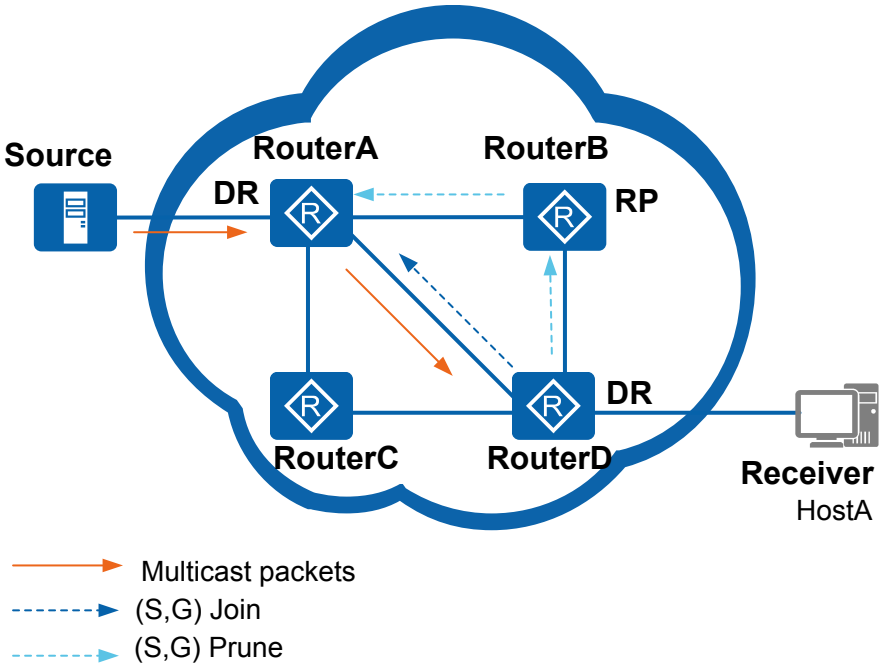
在PIM-SM网络中，一个组播组只对应一个RP，只构建一棵RPT。在未进行SPT切换的情况下，所有发往该组的组播报文都必须先封装在注册报文中发往RP，RP解封装后，再沿RPT分发。RP是所有组播报文必经的中转站，当组播报文速率逐渐变大时，对RP形成巨大的负担。为了解决此问题，PIM-SM允许RP或组成员端DR通过触发SPT切换来减轻RP的负担。

- RP触发SPT切换

  RP收到源端DR的注册报文后，将封装在Register报文中的组播报文沿RPT转发给组成员，同时RP会向源端DR逐跳发送Join报文。发送过程中在PIM路由器创建（S，G）表项，从而建立了RP到源的SPT。

  SPT树建立成功后，源端DR直接将组播报文转发到RP，使源端DR和RP免除了频繁的封装与解封装。
- 组成员端DR触发SPT切换

**图 4-11** 组成员端 DR 触发 SPT 切换示意图




如图4-11所示。组成员端DR周期性检测组播报文的转发速率，一旦发现（S，G）报文的转发速率超过阈值，则触发SPT切换：

a. 组成员端DR逐跳向源端DR逐跳发送Join报文并创建（S，G）表项，建立源端DR到组成员DR的SPT。

b. SPT建立后，组成员端DR会沿着RPT逐跳向RP发送剪枝报文，删除（*，G）表项中相应的下游接口。剪枝结束后，RP不再沿RPT转发组播报文到组成员端。

c. 如果SPT不经过RP，RP会继续向源端DR逐跳发送剪枝报文，删除（S，G）表项中相应的下游接口。剪枝结束后，源端DR不再沿“源端DR-RP”的SPT转发组播报文到RP。

**说明**

缺省情况下，设备一般未设置组播报文转发速率的阈值，RP或者组成员端DR在接收到第一份组播报文时都会触发各自的SPT切换。

## 断言 Assert

断言机制与PIM-DM中的相同，详细内容请参见“PIM-DM断言Assert”。

## BSR 管理域

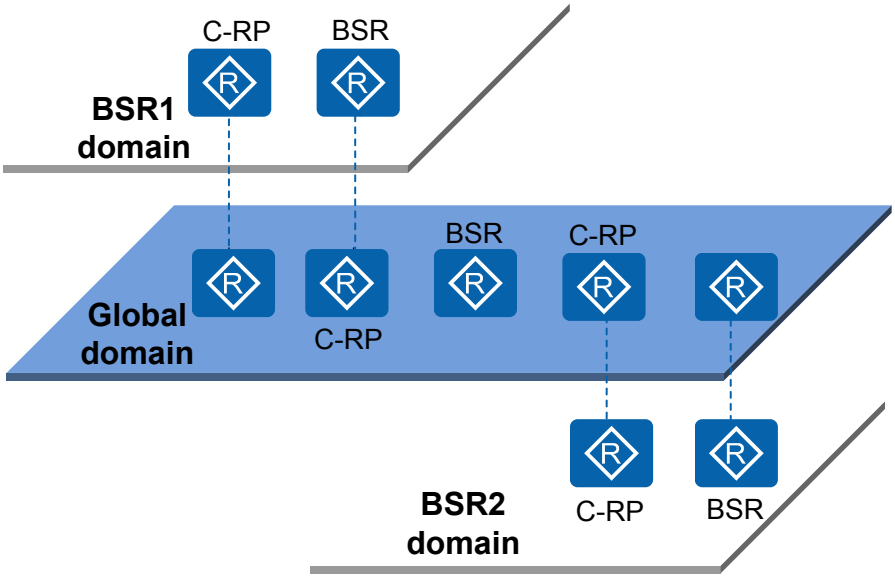
为了实现网络管理精细化，可以选择将一个PIM-SM网络划分为多个BSR管理域和一个Global域。这样一方面可以有效地分担单一BSR的管理压力，另一方面可以使用私有组地址为特定区域的用户提供专门服务。

每个BSR管理域中维护一个BSR，为某一特定地址范围的组播组服务。Global域中维护一个BSR，为所有剩余的组播组服务。

下文将从地域空间、组地址范围、组播功能三个角度分析BSR管理域和Global域的关系。

- 地域空间

**图 4-12** BSR 管理域_地域空间

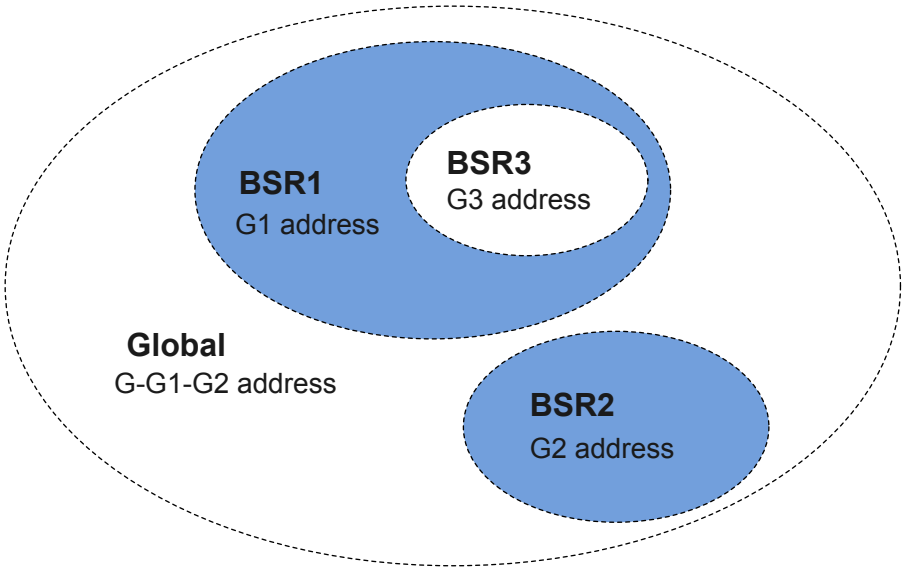



如图4-12所示，对于有相同组地址的不同管理域，各BSR管理域所包含的PIM路由器互不相同，同一PIM路由器不能同时属于多个BSR管理域。各BSR管理域在地域上相互独立，且相互隔离。BSR管理域是针对特定地址范围的组播组的管理区域，属于此范围的组播报文只能在本管理域内传播，无法通过BSR管理域边界。

Global域包含PIM-SM网络内的全部PIM路由器。不属于任意BSR管理域的组播报文，可以在整个PIM网络范围内传播。

- 组地址范围

**图 4-13** BSR 管理域_地址范围




每个BSR管理域为特定地址范围的组播组提供服务，不同的BSR管理域服务的组播组范围可以重叠。该组播地址只在本BSR管理域内有效，相当于私有组地址。如图4-13所示，BSR1域和BSR3域对应的组地址范围出现重叠。

不属于任何BSR管理域的组播组，一律属于Global域的服务范围。如图4-13所示，Global域组地址范围是除G1、G2之外的G-G1-G2。

- 组播功能

  如图4-12所示，Global域和每个BSR管理域都包含针对自己域的C-RP和BSR设备，这些设备在行使相应功能时，仅在本域内有效。即BSR机制和RP竞选在各管理域之间是隔离的。

  每个BSR管理域都有自己的边界，该管理域的组播信息（C-RP宣告报文、BSR自举报文等）不能跨越域传播。同时Global域的组播信息可以在整个Global域内传递，可以穿越任意BSR管理域。

## 4.2.4 PIM-SM（SSM 模型）

### 基本原理

SSM模型是借助PIM-SM的部分技术和IGMPv3/MLDv2来实现的，无需维护RP、无需构建RPT、无需注册组播源，可以直接在源与组成员之间建立SPT。

SSM的特点是网络用户能够预先知道组播源的具体位置。因此用户在加入组播组时，可以明确指定从哪些源接收信息。组成员端DR了解到用户主机的需求后，直接向源端DR发送Join报文。Join报文逐跳向上传输，在源与组成员之间建立SPT。

在SSM模型中，PIM-SM的关键机制包括邻居发现、DR竞选、构建SPT。

### 邻居发现

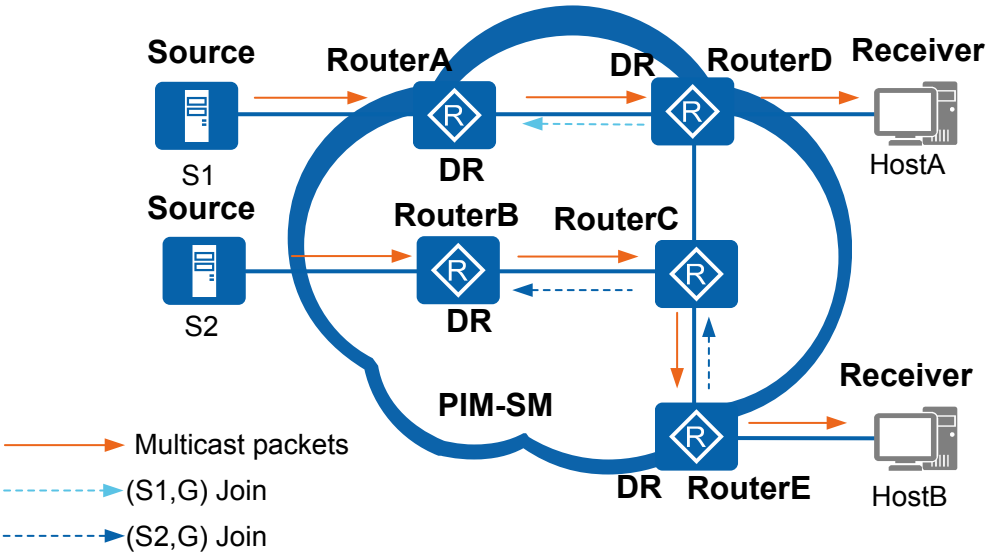
邻居发现机制与PIM-DM中的相同，详细内容请参见“PIM-DM 邻居发现”。

### DR 竞选

DR竞选机制与PIM-SM（ASM模型）中的相同，详细内容请参见“PIM-SM（ASM模型） DR竞选”。

### SPT 构建

**图 4-14** SPT 构建示意图



如图1所示，SPT的建立过程如下：

1. RouterD、RouterE借助IGMPv3/MLDv2协议了解到用户主机有到相同组播组不同组播源的组播需要，逐跳向源方向发送Join报文。
2. PIM路由器通过Join报文分别创建（S1，G）、（S2，G）表项，从而分别建立了源S1到组成员HostA、源S2到组成员HostB的SPT。
3. SPT建立后，源端就会将组播报文沿着SPT分发给组成员。

### 与 ASM 模型比较

SSM模型与ASM模型之间的最大差异就是是否指定了组播源，具体的区别如表1。

**表 4-1** PIM 实现方式比较

| 协议 | 名称 | 模型分类 | 适用场景 | 工作机制 |
| --- | --- | --- | --- | --- |
| PIM-DM | Protocol Independent Multicast-Dense Mode 协议无关组播—密集模式 | ASM模型 | 适合规模较小、组播组成员相对比较密集的局域网。 | 通过周期性“扩散-剪枝”维护一棵连接组播源和组成员的单向无环SPT。 |
| PIM-SM | Protocol Independent Multicast-Sparse Mode 协议无关组播—稀疏模式 | ASM模型 | 适合网络中的组成员相对比较稀疏，分布广泛的大型网络。 | 采用接收者主动加入的方式建立组播分发树，需要维护RP、构建RPT、注册组播源。 |
| | | SSM模型 | 适合网络中的用户预先知道组播源的位置，直接向指定的组播源请求组播数据的场景。 | 直接在组播源与组成员之间建立SPT，无需维护RP、构建RPT、注册组播源。 |

## 4.2.5 PIM BFD

为了减小设备故障对业务的影响，提高网络的可靠性，网络设备需要快速检测到与相邻设备间的通信故障，以便及时采取措施，保证业务继续进行。

BFD（Bidirectional Forwarding Detection）检测机制可提供毫秒级的快速检测，并采用单一机制对所有类型的介质、协议层进行检测，实现全网统一的检测机制。其检测原理是在两个系统间建立BFD会话，并沿它们之间的路径周期性发送BFD检测报文，如果一方在检测周期内没有收到BFD检测报文，则认为该路径发生了故障。

### 基本原理

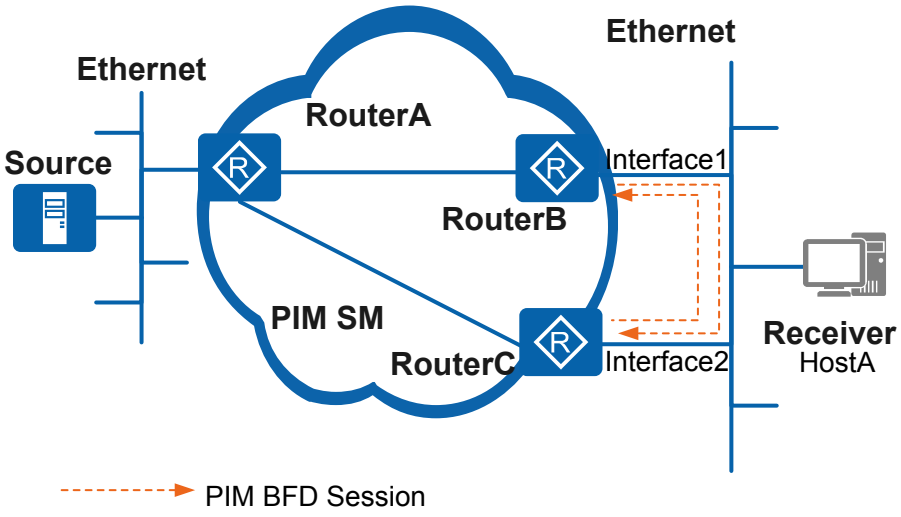
在组播的应用中，如果共享网段上的当前DR或Assert winner发生故障，其他PIM邻居会等到邻居关系超时或Assert timer超时才触发新一轮的DR竞选或Assert竞选过程，导致

组播数据传输中断，中断的时间将不小于邻居关系的超时时间或Assert timer超时时间，通常是秒级。

PIM BFD能够在毫秒级内检测共享网段内的链路状态，快速响应PIM邻居故障。如果配置了PIM BFD功能的接口在检测周期内没有收到当前DR或Assert winner发送的BFD检测报文，则认为当前DR或Assert winner发生故障，BFD快速把会话状态通告给RM，再由RM通告给PIM。PIM模块触发新一轮的DR竞选或Assert竞选过程，而不是等到邻居关系超时或Assert timer超时，从而缩小组播数据传输的中断时间，提高组播数据传输的可靠性。

**图 4-15** PIM BFD 原理图




如图1所示，在与用户主机相连的共享网段上，RouterB的下游接口Interface1和RouterC的下游接口Interface2之间建立PIM BFD会话，通过在链路两端发送BFD检测报文检测链路状态。

RouterB作为当前DR，下游接口Interface1负责接收端组播数据的转发。若接口Interface1发生故障，BFD快速把会话状态通告给RM，再由RM通告给PIM。PIM模块触发新一轮的DR竞选，RouterC作为新当选的DR，下游接口Interface2在短时间内向接收端转发组播数据，从而缩小组播数据传输的中断时间。

## 4.2.6 PIM GR

平滑重启GR（Graceful Restart）属于高可靠性HA（High Availability）技术的一种，实现协议重启时业务的不间断转发（Multicast Non-Stop Forwarding）能力。PIM GR是一种组播协议GR。在具有双主控板的设备上，PIM GR可以在设备进行主备倒换时实现用户组播流量的正常转发。

目前，仅PIM-SM（ASM模型）与PIM-SM（SSM模型）支持PIM GR，PIM-DM不支持PIM GR。

**说明**

仅AR3200系列支持PIM GR。

## 基本原理

PIM GR依赖于单播GR。设备进行主备倒换期间，新主控板的PIM协议需要从下游邻居重新学习PIM加入状态，同时还需要从IGMP成员主机学习加入的组成员。新主控板的PIM协议通过以上过程完成如下动作：

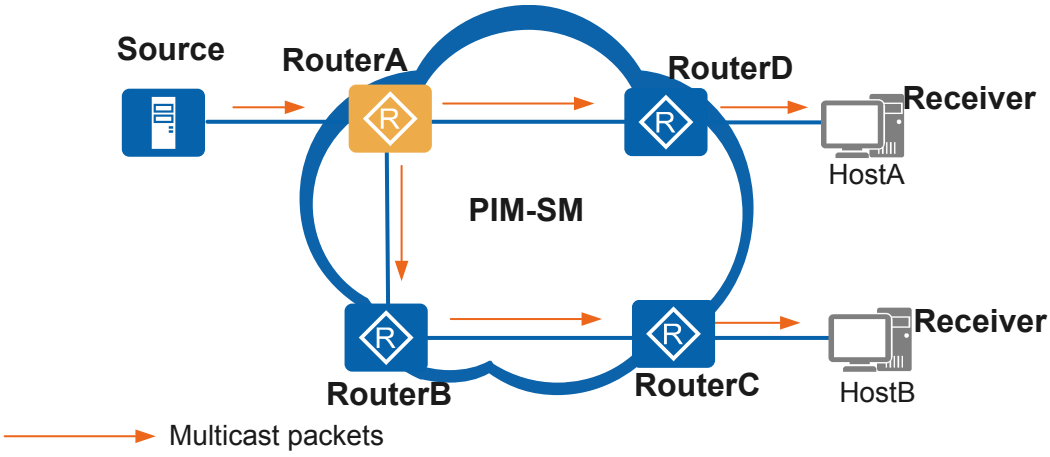
- 重新计算PIM组播路由表项。
- 维持下游邻居的加入状态。
- 更新转发平面的组播路由表项。

通过PIM GR，设备可以达到主备倒换后快速恢复新的主用主控板的PIM路由表项及刷新接口板组播转发表项的目的，从而最大限度地减少主备倒换对用户组播流量转发的影响。

## 工作机制

如图1所示，介绍RouterA进行PIM GR的过程。

**图 4-16** PIM GR 示意图




PIM GR建立在单播GR的基础上，整个PIM GR的过程分为三个阶段：开始阶段（GR_START）、同步阶段（GR_SYNC）和完成阶段（GR_END）。

**GR_START**

1. RouterA发生主备倒换，PIM协议启动GR定时器，PIM GR进入开始阶段，同时单播开始进行GR。
2. PIM协议向所有使能PIM-SM的接口发送携带新的Generation ID的Hello报文。
3. RouterA的下游邻居RouterB、RouterD发现RPF邻居的Generation ID改变，向RouterA重新发送Join/Prune报文。
4. 若网络中使用动态RP，当网络中的邻居收到Generation ID改变的Hello报文后，向RouterA单播发送BSR报文，恢复RouterA的BSR及RP信息。
5. RouterA通过接收下游RouterB、RouterD发送的Join/Prune报文，在空的入接口表中创建PIM路由表项，记录下游的加入信息。

   在此期间，转发模块转发表项保持不变，维持组播业务数据的转发。

**GR_SYNC**

单播GR结束，PIM GR进入同步阶段，根据单播路由信息建立组播分发树，恢复PIM路由表项的入接口，更新到源或到RP的加入队列，并通知组播转发模块更新转发表。

**GR_END**

GR定时器超时，PIM协议完成GR，并通知组播转发模块。组播转发模块老化GR期间未更新的转发表项。

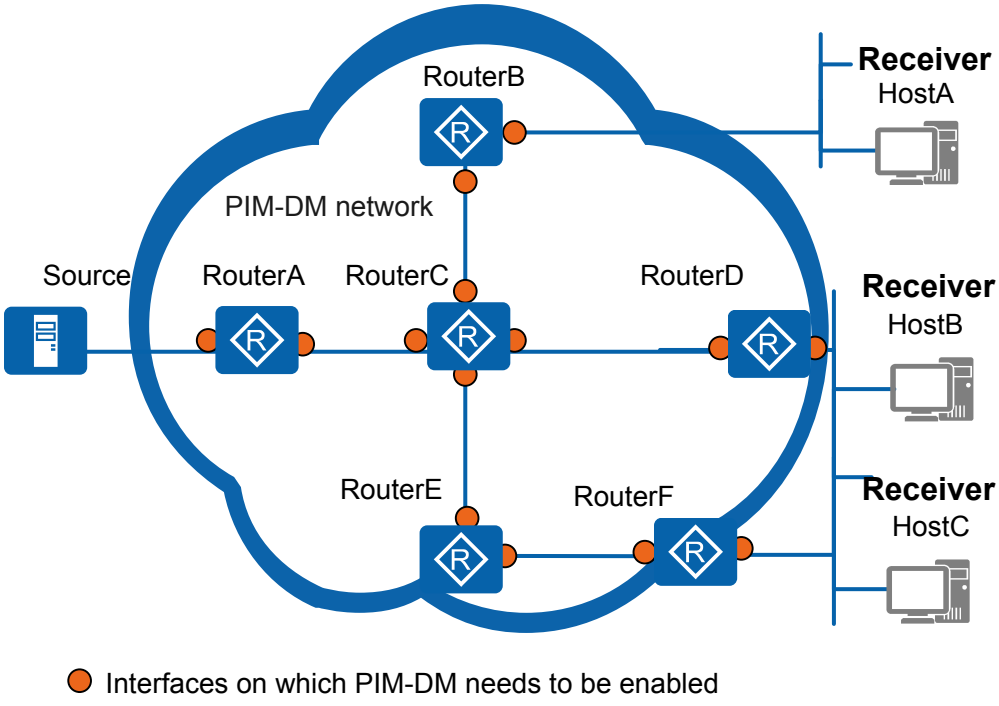
# 4.3 PIM 应用场景

介绍组播PIM协议的应用场景。

## 4.3.1 单自治域 PIM-DM 应用

在如图1所示的小型网络中部署组播业务。该网络中已经部署了完备的IGP，且任意网段路由可达。网络中的组成员分布相对比较密集，要求网络中的用户主机能够按需接收视频点播信息，并在一定程度上节约网络的带宽。

**图 4-17** 单自治域 PIM-DM 应用组网图




### 实现方案

如图1所示，HostA、HostB和HostC为网络中的信息接收者，通过组播方式接收视频点播信息，整个PIM域采用PIM-DM方式。RouterA与组播源Source相连；RouterB连接HostA，RouterD和RouterF连接HostB和HostC。

网络部署如下：

- 在所有路由器接口上启用PIM-DM协议。
- RouterB与HostA之间，RouterD、RouterF与HostB、HostC之间均运行IGMP协议。

为路由器接口配置IGMP协议时，请确保接口参数配置的一致性，即遵循如下原则：连接在同一网段的所有路由器必须运行相同的IGMP版本（推荐使用IGMPv2），且各接口参数（如查询定时器、组成员关系保持时间等）必须相同。如果IGMP版本或各参数不相同，会导致不同路由器上IGMP组成员关系不一致。

- 部署完上述网络后，HostA、HostB和HostC能够接收到组播源的数据，正常收看视频点播信息。

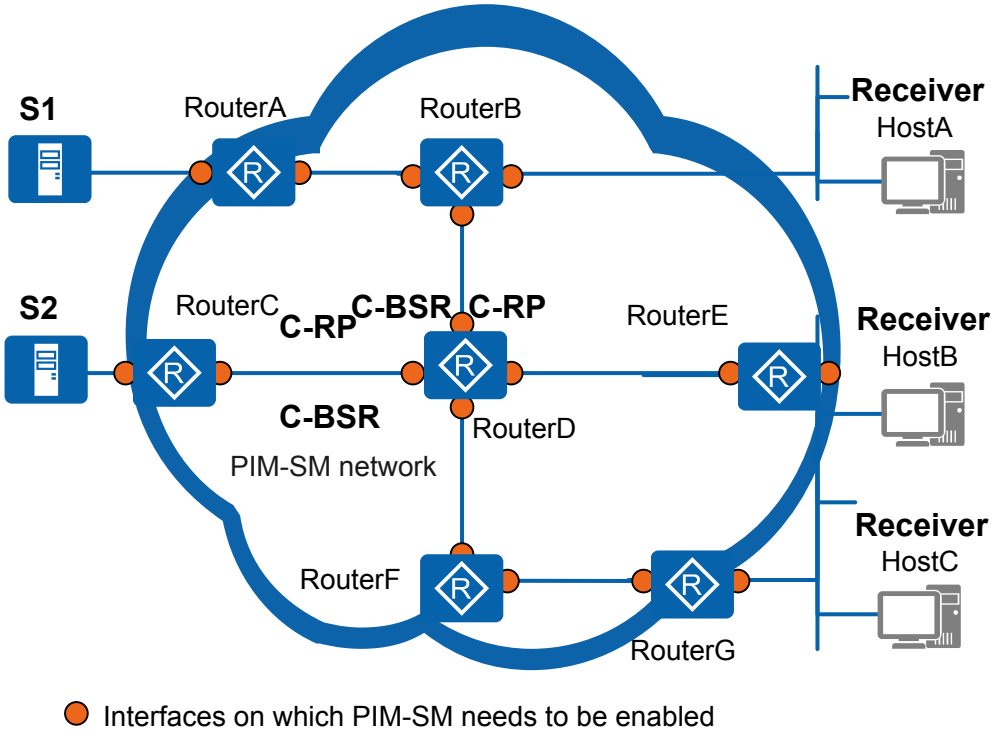
  **说明**

  建议在网络边缘配置接口静态加入用户所请求的组播组，可以提高用户收看频道的稳定性。

## 4.3.2 单自治域 PIM-SM 应用

在如图1所示的大型网络中部署组播业务。该网络中已经部署了完备的IGP，且任意网段路由可达。网络中的组成员分布相对比较稀疏，要求网络中的用户主机能够按需接收视频点播信息，并在一定程度上节约网络的带宽。

**图 4-18** 单自治域 PIM-SM 应用组网图




### 实现方案

如图1所示，HostA、HostB和HostC为网络中的信息接收者，通过组播方式接收视频点播信息，整个PIM域采用PIM-SM方式。RouterA与组播源S1相连，RouterC与组播源S2相连；RouterB连接HostA，RouterE和RouterG连接HostB和HostC。

网络部署如下：

- 在所有路由器接口上启用PIM-SM协议。
- 如图1所示，网络中的组播源分布比较密集，则可以选择与组播源比较近的核心设备作为C-RP。将RouterC和RouterD的接口配置为C-BSR和C-RP，动态竞选出为PIM-SM网络服务的BSR和RP。

RP部署方式的选择：

- 中小型网络：建议选择静态RP方式，对设备要求低，也比较稳定。

  如果网络中只有一个组播源，建议选择直连组播源的设备作为静态RP，这样可以省略源端DR向RP注册的过程。

  采用静态RP方式要确保域内所有路由器（包括RP本身）的RP信息以及服务的组播组范围全网一致。
- 大型网络：可以采用动态RP方式，可靠性高，可维护性强。

  如果网络中存在多个组播源，且分布密集，建议选择与组播源比较近的核心设备作为C-RP；如果网络中存在多个用户，且分布密集，建议选择与用户比较近的核心设备作为C-RP。

**说明**

避免在一个PIM域中不同路由器上分别使用静态RP和动态RP，以防止RP信息不一致。

- RouterB与HostA之间，RouterE、RouterG与HostB、HostC之间均运行IGMP协议。

  为路由器接口配置IGMP协议时，请确保接口参数配置的一致性，即遵循如下原则：连接在同一网段的所有路由器必须运行相同的IGMP版本（推荐使用IGMPv2），且各接口参数（如查询定时器、组成员关系保持时间等）必须相同。如果IGMP版本或各参数不相同，会导致不同路由器上IGMP组成员关系不一致。
- 部署完上述网络后，HostA、HostB和HostC根据需要向RP发送Join消息，组播源的信息能够到达接收者。

**说明**

建议在网络边缘配置接口静态加入用户所请求的组播组，可以提高用户收看频道的稳定性。

# 4.4 配置 PIM（IPv4）任务概览

PIM协议配置完成后，就可实现组播数据在IPv4网络的组播路由与转发。PIM协议包含多种不同类型的模式，不同模式的PIM协议适用于不同的应用场景。

PIM的配置任务如表4-2所示。

**表 4-2** PIM 配置任务概览

| 场景 | 描述 | 对应任务 |
| --- | --- | --- |
| 配置PIM-DM | PIM-DM协议使用ASM模型提供组播服务。配置简单，但是组播数据会周期性的在全网扩散，适合规模较小、组播组成员相对比较密集的网络。 | 4.7 配置PIM-DM（IPv4） |

| 场景 | 描述 | 对应任务 |
| --- | --- | --- |
| 配置PIM-SM | PIM-SM协议使用ASM模型和SSM模型提供组播服务。对于ASM模型，采用接收者主动加入的方式建立组播分发树，需要维护RP、构建RPT、注册组播源，适合网络中的组成员相对比较稀疏，分布广泛的大型网络；对于SSM模型，采用PIM-SM技术，直接在组播源与组成员之间建立SPT，无需维护RP、构建RPT、注册组播源，适合网络中的用户预先知道组播源的位置，直接向指定的组播源请求组播数据的场景。 | 4.8 配置PIM-SM（IPv4） |
| 配置PIM多实例 | PIM多实例是指在VPN实例下配置PIM协议。路由器通过配置PIM多实例，就可以实现私网组播数据在VPN实例内组播路由与转发。并且各个VPN实例间配置的PIM协议互不影响。 | PIM多实例的相关配置，已经包含在本章的所有配置任务中。 |

# 4.5 PIM（IPv4）配置注意事项

介绍配置PIM（IPv4）的注意事项。

## 涉及网元

一个完整的IPv4组播网络涉及以下网元：

- 组播源：发送组播数据给组播用户主机，比如视频服务器。
- 运行PIM（IPv4）协议的设备：通过PIM（IPv4）协议生成组播路由表项，转发组播数据。在组播网络里，所有三层设备上都需要运行PIM（IPv4）协议，否则组播转发路径无法正常建立。
- 运行MSDP协议的设备：实现跨PIM网络的组播数据转发，所以主要应用在网络规模大的场合。比如两个AS系统需要实现组播通信，就在AS间的边缘设备上运行MSDP协议。
- IGMP查询器：与组播用户主机之间交互IGMP报文，建立和维护组播组成员关系。在组播网络里，连接用户侧的三层设备都需要运行IGMP协议或者静态配置IGMP组播组，否则上游运行PIM协议的设备无法了解到用户需求，组播转发路径无法正常建立。
- 运行IGMP Snooping的设备：通过侦听上游三层组播设备与组播用户主机之间交互的IGMP报文，生成二层组播转发表项，指导组播数据在二层网络的精确转发。为

了避免组播报文二层网络广播，减少带宽浪费，建议在二层设备上配置IGMP Snooping功能。

- 接收者：接收组播数据的组播用户。接收者可以为PC、机顶盒等，但是需要具备相应的组播客户端软件。

## License 支持

PIM（IPv4）是路由器的基本特性，无需获得License许可应用此功能。

## 特性依赖和限制

在路由器上部署PIM功能时需注意：VPN实例或者公网实例上不能同时使能PIM-DM和PIM-SM。

**说明**

AR120系列不支持此功能。

# 4.6 PIM（IPv4）缺省配置

介绍缺省情况下，PIM的配置信息。

表4-3列出了PIM的缺省配置。

**表 4-3** PIM 的缺省配置

| 参数 | 缺省值 |
| --- | --- |
| 组播路由功能 | 未使能 |
| PIM-DM | 未使能 |
| 状态刷新功能 | PIM-DM使能后，该功能默认已使能 |
| PIM-SM | 未使能 |
| 静态RP地址 | 未配置 |
| C-RP接口 | 未指定 |
| C-BSR接口 | 未指定 |
| Auto-RP侦听功能 | 未使能 |
| DR优先级 | 1 |
| SPT切换条件 | RP或组成员端DR接收到第一个组播数据报文时就进行SPT切换 |
| SSM组地址范围 | 232.0.0.0/8 |
| PIM BFD | 未使能 |
| PIM GR | 未使能 |
| PIM Silent | 未使能 |

# 4.7 配置 PIM-DM（IPv4）

通过配置PIM-DM协议，可以实现域内组播路由与数据转发。PIM-DM是密集模式的域内组播路由协议，适用于组成员分布相对集中、范围较小的网络。

## 4.7.1 配置 PIM-DM 基本功能

PIM-DM网络的所有设备使能了PIM-DM后，就可为用户主机提供任意源组播服务，加入同一组播组的用户主机都能收到任意源发往该组的组播数据。

### 前置任务

配置单播路由协议，保证网络内单播路由畅通。

### 背景信息

VPN实例或者公网实例上不能同时使能PIM-DM和PIM-SM。

建议将处于PIM-DM网络内的所有接口都使能PIM-DM，以确保与其相连的PIM设备都能建立邻居关系。

如果接口上需要同时使能PIM-DM和IGMP，必须要先使能PIM-DM，再使能IGMP。

### 操作步骤

- 使能公网实例的PIM-DM
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**multicast routing-enable**，使能组播路由功能。
  c. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  d. 执行命令**pim dm**，使能PIM-DM功能。
- 使能VPN实例的PIM-DM

  使能VPN实例的PIM-DM之前，应该已经创建好VPN实例。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**ip vpn-instance** *vpn-instance-name*，进入VPN实例视图。
  c. 执行命令**multicast routing-enable**，使能组播路由功能。
  d. 执行命令**quit**，退回系统视图。
  e. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  f. 执行命令**ip binding vpn-instance** *vpn-instance-name*，将接口与VPN实例进行关联。
  g. 执行命令**pim dm**，使能PIM-DM功能。

**----结束**

### 检查配置结果

在PIM域内的所有设备上都使能了PIM-DM之后，可以通过命令查看PIM接口、PIM邻居和PIM路由表等信息。

- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]，查看接口上的PIM信息。
- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **neighbor** [ *neighbor-address* | **interface** *interface-type interface-number* | **verbose** ] *，查看PIM邻居信息。
- 使用以下命令查看PIM路由表：
  - 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm** ] * [ **outgoing-interface-number** [ *number* ] ]，查看PIM路由表详细信息。
  - 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table brief** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } ] *，查看PIM路由表简要信息。

## 4.7.2 调整组播源控制参数

通过ACL对组播源的地址进行过滤，以及对组播源生存时间进行控制，可以提高数据安全性、控制网络流量。

### 前置任务

在调整组播源控制参数之前，需完成以下任务：

**4.7.1 配置PIM-DM基本功能**

### 背景信息

当PIM设备在接收到源S发往组播组G的组播报文后，就会启动该（S，G）表项的定时器，时间设为源生存时间。如果超时前接收到源S后续发来的报文，则重置定时器；如果超时后没有接收到源S后续发来的报文，则认为（S，G）表项失效，将其删除。

如果希望控制组播流量或者保证接收数据的安全性，还可在PIM设备上配置源地址过滤策略，只接收该策略允许范围内组播源发送的组播数据。

### 缺省配置

表4-4列出了组播源控制参数的缺省配置。

**表 4-4 组播源控制参数的缺省配置**

| 参数 | 缺省值 |
| --- | --- |
| 组播源生存时间 | 210s |
| 源地址过滤策略 | 没有过滤策略，即接收任何组播源发来的组播数据。 |

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

**步骤3** 执行命令**source-lifetime** *interval*，配置组播源生存时间。

**步骤4** 执行命令**source-policy** { *acl-number* | **acl-name** *acl-name* }，配置源地址过滤策略。

- 如果配置的是基本ACL，通过与**rule**中的**source**参数配合，只转发源地址属于过滤规则允许范围的组播报文。
- 如果配置的是高级ACL，通过与**rule**中的**source**和**destination**参数配合，只转发源地址和组地址都属于过滤规则允许范围内的组播报文。
- 如果指定ACL没有配置过滤规则，则不转发任何源地址发送的组播报文。
- 执行本功能不过滤静态（S，G）和记录了私网加入信息的PIM表项。

**----结束**

## 检查配置结果

使用如下命令查看PIM路由表中的表项是否符合要求。

- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm** ] * [ **outgoing-interface-number** [ *number* ] ]，查看PIM路由表详细信息。
- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table brief** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } ] *，查看PIM路由表简要信息。

# 4.7.3 调整邻居控制参数

通过调整邻居控制参数，控制邻居间Hello报文的交互，可以防止非法邻居关系的建立，保证PIM-DM网络的安全。

## 前置任务

在调整邻居控制参数之前，需完成以下任务：

**4.7.1 配置PIM-DM基本功能**

## 配置流程

调整Hello报文的时间控制参数、配置邻居过滤策略在配置时并无先后顺序，可根据实际需要进行调整。

### 4.7.3.1 调整 Hello 报文的时间控制参数

## 背景信息

PIM设备通过周期性地发送Hello报文来维护PIM邻居关系。当PIM设备收到邻居发来Hello报文后，会启动定时器，时间设为该Hello报文的保持时间。如果超时后没有收到邻居发来的Hello报文，则认为该邻居失效或者不可达。因此，PIM设备发送Hello报文的时间间隔必须要小于Hello报文的保持时间。

为了避免多个PIM设备同时发送Hello报文而导致冲突，当PIM设备接收到Hello报文时，将延迟一段时间再发送Hello报文。该段时间的值为一个随机值，并且小于触发Hello报文的最大延迟。

**说明**

- 发送Hello报文的时间间隔、Hello报文的保持时间在全局PIM视图下和接口视图下都可配置。如果同时配置，接口视图上的配置生效。
- 触发Hello报文的最大延迟时间只能在接口上配置。

## 缺省配置

表4-5列出了Hello报文时间参数的缺省配置。

**表 4-5** Hello 报文时间参数的缺省配置

| 参数 | 缺省值 |
| --- | --- |
| 发送Hello报文的时间间隔 | 30s |
| Hello报文的保持时间 | 105s |
| 触发Hello报文的最大延迟时间 | 5s |

## 操作步骤

- 全局配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**timer hello** *interval*，配置发送Hello报文的时间间隔。
  d. 执行命令**hello-option holdtime** *interval*，配置Hello报文的保持时间。
- 接口配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**pim timer hello** *interval*，配置发送Hello报文的时间间隔。
  d. 执行命令**pim hello-option holdtime** *interval*，配置Hello报文的保持时间。
  e. 执行命令**pim triggered-hello-delay** *interval*，配置触发Hello报文的最大延迟。

**----结束**

## 4.7.3.2 配置邻居过滤策略

## 背景信息

设备支持不同的邻居过滤策略，来保证PIM-DM网络的安全和畅通：

- 限定合法的邻居地址范围，防止非法邻居入侵等。
- 拒绝接收无Generation ID的Hello报文，保证设备相连的都是正常工作的PIM邻居。

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**interface** *interface-type interface-number*，进入接口视图。

**步骤3** 执行命令**pim neighbor-policy** { *basic-acl-number* | **acl-name** *acl-name* }，配置合法的邻居地址范围。

**说明**

- 设备上配置了合法的邻居地址范围后，如果之前与其建立好邻居关系的PIM设备不在其合法地址范围内，后续将不会再收到邻居设备的Hello报文。邻居关系也会因Hello报文的保持时间超时而解除。

**步骤4** 执行命令**pim require-genid**，配置只接收包含Generation ID的Hello报文。

缺省情况下，PIM接口接收无Generation ID参数的Hello报文。

**----结束**

### 4.7.3.3 检查配置邻居控制参数的结果

## 前提条件

调整邻居控制参数后，可使用以下命令查看PIM接口和PIM邻居是否符合要求。

## 操作步骤

- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]，查看接口上的PIM信息。
- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **neighbor** [ *neighbor-address* | **interface** *interface-type interface-number* | **verbose** ] *，查看PIM邻居信息。

**----结束**

# 4.7.4 调整剪枝控制参数

设备向上游发送Prune信息请求停止转发组播数据。可以根据不同场景需要调整剪枝控制参数，若无特殊需要，推荐使用缺省值。

## 前置任务

在调整剪枝控制参数之前，需完成以下任务：

**4.7.1 配置PIM-DM基本功能**

## 配置流程

Join/Prune报文的时间控制参数、Join/Prune报文的信息携带能力、剪枝延迟时间配置时无先后顺序，用户可根据实际需要进行调整。

### 4.7.4.1 调整 Join/Prune 报文的时间控制参数

## 背景信息

PIM设备通过向上游发送Prune信息请求停止转发组播数据。实际上，Prune信息被封装在了PIM协议通用的转发控制报文（即Join/Prune报文）中。上游设备在收到Join/Prune报文后，就会启动定时器，时间设为Join/Prune报文自身携带的保持时间。超时后，如果没有收到下游后续发来的Join/Prune报文，则恢复相应组播组下游接口的转发。

**说明**

Join/Prune报文的保持时间在全局PIM视图下和接口视图下都可配置，如果同时配置，接口视图上的配置生效。

## 缺省配置

表4-6列出了Join/Prune报文时间参数的缺省配置。

**表 4-6** Join/Prune 报文时间参数的缺省配置

| 参数 | 缺省值 |
| --- | --- |
| Join/Prune报文的保持时间 | 210s |

## 操作步骤

- 全局配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**holdtime join-prune** *interval*，配置Join/Prune报文的保持时间。
- 接口配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**pim holdtime join-prune** *interval*，配置Join/Prune报文的保持时间。

**----结束**

### 4.7.4.2 调整 Join/Prune 报文的信息携带能力

## 背景信息

在PIM-DM网络，Join/Prune报文主要包含了需要剪枝的表项信息。设备支持通过配置Join/Prune报文长度、包含表项数目、发送方式，来调整向上游发送剪枝信息的信息量：

- 当PIM邻居设备性能比较差，处理单个Join/Prune报文耗时比较长，可以通过调整发送的Join/Prune报文长度来控制发送Join/Prune报文携带的(S, G)表项数量，来降低PIM邻居设备的压力。
- 当PIM邻居设备Join/Prune报文处理吞吐量比较小时，可以通过调整周期性报文发送队列长度，控制每次发给PIM邻居设备的(S, G)表项数量，采取小量多批次方式发送Join/Prune报文，从而避免PIM邻居设备来不及处理就将报文丢弃，引起路由振荡。
- 缺省情况下，为了提高发送效率，Join/Prune报文都是打包向上游发送。如果不希望Join/Prune报文打包发送，可去使能此功能。

## 缺省配置

表4-7列出了Join/Prune报文部分参数的缺省配置。

**表 4-7** Join/Prune 报文部分参数的缺省配置

| 参数 | 缺省值 |
| --- | --- |
| Join/Prune报文长度 | 8100字节 |
| Join/Prune报文包含的表项数目 | 1020个 |
| Join/Prune报文的发送方式 | 打包发送 |

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

**步骤3** 执行命令**join-prune max-packet-length** *packet-length*，配置设备发送的Join/Prune报文的最大长度。

**步骤4** 执行命令**join-prune periodic-messages queue-size** *queue-size*，配置设备每秒发送Join/Prune报文中包含的表项数目。

**步骤5** 执行命令**join-prune triggered-message-cache disable**，去使能实时触发的Join/Prune报文打包功能。

**----结束**

## 4.7.4.3 调整剪枝延迟时间

## 背景信息

在剪枝过程中，从收到下游设备发来的剪枝信息到继续向上游设备发送剪枝信息会有延迟时间，这段时间称为LAN-Delay。PIM设备在向上游发完剪枝信息后，也不会立即将相应下游接口剪掉，还会保持一段时间向下游转发。如果下游又有组播需求，必须要在这段时间内发送加入请求以否决这个剪枝动作。这段否决剪枝的时间称为Override-Interval。所以，实际上PIM设备从收到剪枝信息到完成剪枝动作总共延迟了LAN-Delay＋Override-Interval段时间。

**说明**

LAN-Delay、Override-Interval在全局PIM视图下和接口视图下都可配置，如果同时配置，接口视图下的配置生效。

## 缺省配置

表4-8列出了剪枝延迟时间参数的缺省配置。

**表 4-8 剪枝延迟时间参数的缺省配置**

| 参数 | 缺省值 |
| --- | --- |
| LAN-Delay | 500ms |
| Override-Interval | 2500ms |

## 操作步骤

- 全局配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**hello-option lan-delay** *interval*，配置发送剪枝报文的延迟时间。
  d. 执行命令**hello-option override-interval** *interval*，配置否决剪枝的时间。
- 接口配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**pim hello-option lan-delay** *interval*，配置发送剪枝报文的延迟时间。
  d. 执行命令**pim hello-option override-interval** *interval*，配置否决剪枝的时间。

**----结束**

## 4.7.4.4 检查配置调整剪枝控制参数的结果

## 前提条件

调整剪枝控制参数成功后，可以通过命令查看PIM接口、PIM控制消息统计数和PIM路由表等信息。

## 操作步骤

- 执行命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]，查看接口上的PIM信息。
- 执行命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **control-message counters** [ **message-type** { **assert** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** | **bsr** } | **interface** *interface-type interface-number* ] *，查看发送和接收PIM控制报文的数目信息。
- 使用以下命令查看PIM路由表：
  - 执行命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm** ] * [ **outgoing-interface-number** [ *number* ] ]，查看PIM路由表详细信息。
  - 执行命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table brief** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } ] *，查看PIM路由表简要信息。

**----结束**

# 4.7.5 调整嫁接控制参数

当被剪枝的网段出现新的组成员，设备可以通过向上游发送嫁接（Graft）报文使该网段快速的恢复转发。通过调整嫁接控制参数，可以控制组播数据报文的转发来支持不同转发场景。

## 前置任务

在调整嫁接控制参数之前，需完成以下任务：

**4.7.1 配置PIM-DM基本功能**

## 背景信息

为使被剪枝网段快速恢复转发，设备会向上游发送Graft报文请求恢复组播数据转发，并同时在发送接口启动定时器。超时后，如果设备仍没有接收到组播数据，会重新向上游发送Graft报文。

## 缺省配置

表4-9列出了嫁接控制参数的缺省配置。

**表 4-9 嫁接控制参数的缺省配置**

| 参数 | 缺省值 |
| --- | --- |
| Graft报文重传的时间间隔 | 3s |

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**interface** *interface-type interface-number*，进入接口视图。

**步骤3** 执行命令**pim timer graft-retry** *interval*，配置Graft报文重传的时间间隔。

**----结束**

## 检查配置结果

调整嫁接控制参数成功后，可以通过命令查看PIM-DM嫁接、PIM接口等信息是否符合要求。

- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]，查看接口上的PIM信息。
- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **grafts**，查看未确认的PIM-DM嫁接信息。

# 4.7.6 调整状态刷新控制参数

为防止被剪枝接口因为剪枝状态超时而恢复转发，PIM-DM网络启用了状态刷新功能，通过与组播源直连的第一跳PIM设备周期性的扩散发送State-Refresh报文，刷新接口剪枝定时器，维持SPT树。

## 前置任务

在调整状态刷新控制参数之前，需完成以下任务：

**4.7.1 配置PIM-DM基本功能**

## 配置流程

禁止状态刷新报文的转发、调整状态刷新报文的时间控制参数、配置状态刷新报文的TTL值配置时无先后顺序，用户可根据实际需要进行调整。

### 4.7.6.1 禁止状态刷新报文的转发

## 背景信息

为了避免下游一直没有组播需求的被剪枝接口因为超时而恢复转发，与组播源S直连的PIM设备会触发发送（S，G）状态刷新报文。该报文会逐跳向下游扩散，刷新所有PIM设备上的剪枝定时器。这样没有转发需求的接口将一直处于抑制转发状态。

缺省情况下，设备都具备状态刷新报文的转发能力。如果希望组播数据每一次“扩散-剪枝”时都能在全网扩散，不需要通过设备转发状态刷新报文来抑制被剪枝接口转发组播数据，可在接口上禁止此功能。

**说明**

状态刷新机制能够很好的减少网络资源浪费，一般情况下不建议禁止接口的状态刷新报文的收发能力。

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**interface** *interface-type interface-number*，进入接口视图。

**步骤3** 执行命令**undo pim state-refresh-capable**，禁止状态刷新报文的转发。

缺省情况下，接口允许状态刷新报文的转发。

禁止了状态刷新报文的转发后，可在接口上执行命令**pim state-refresh-capable**重新启用此功能。

**----结束**

## 4.7.6.2 调整状态刷新报文的时间控制参数

## 背景信息

与组播源直连的第一跳PIM设备会周期性的向下游发送状态刷新报文。由于状态刷新报文扩散发送，设备很有可能在短时间内收到重复的状态刷新报文。为了避免这种情况发生，设备在收到针对某（S，G）的状态刷新报文后，就会启动定时器，时间设为该报文的抑制时间。在定时器超时前，如果收到相同的状态刷新报文，就会直接丢弃。

## 缺省配置

表4-10列出了状态刷新报文时间控制参数的缺省配置。

**表 4-10 状态刷新报文时间控制参数的缺省配置**

| 参数 | 缺省值 |
| --- | --- |
| 状态刷新报文的发送周期 | 60s |
| 相同状态刷新报文抑制时间 | 30s |

## 操作步骤

- 在与组播源直接相连的第一跳设备上配置状态刷新报文的发送周期
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**state-refresh-interval** *interval*，配置状态刷新报文的发送周期。
- 在所有设备上配置相同状态刷新报文抑制时间
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**state-refresh-rate-limit** *interval*，配置相同状态刷新报文的抑制时间。

**----结束**

### 4.7.6.3 配置状态刷新报文的 TTL 值

## 背景信息

设备在收到状态刷新报文后，会将状态刷新报文的TTL值减1，然后继续向下游扩散转发来刷新下游设备的剪枝定时器，直至状态刷新报文的TTL值为0。当网络规模很小而TTL值很大时，会造成状态刷新报文在网络中循环传递。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配置合适的TTL值。

**说明**

因为状态刷新报文是由与组播源直连的第一跳PIM设备触发发送，所以状态刷新报文的TTL值只在该设备上配置有效。

## 缺省配置

表4-11列出了状态刷新报文TTL值的缺省配置。

**表 4-11** 状态刷新报文 TTL 值的缺省配置

| 参数 | 缺省值 |
| --- | --- |
| 状态刷新报文的TTL值 | 255 |

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

**步骤3** 执行命令**state-refresh-ttl** *ttl-value*，配置转发状态刷新报文的TTL值。

**----结束**

### 4.7.6.4 检查配置调整状态刷新控制参数的结果

## 前提条件

调整状态刷新控制参数成功后，可以通过命令查看PIM接口、PIM控制消息统计数和PIM路由表等信息。

## 操作步骤

- 执行命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]，查看接口上的PIM信息。
- 执行命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **control-message counters** [ **message-type** { **assert** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** | **bsr** } | **interface** *interface-type interface-number* ] *，查看发送和接收PIM控制报文的数目信息。
- 使用以下命令查看PIM路由表：

- 执行命令**display pim [ vpn-instance** *vpn-instance-name* | **all-instance ] routing-table [** *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm** ] * [ **outgoing-interface-number** [ *number* ] ]，查看PIM路由表详细信息。
- 执行命令**display pim [ vpn-instance** *vpn-instance-name* | **all-instance ] routing-table brief [** *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } ] *，查看PIM路由表简要信息。

**----结束**

# 4.7.7 调整断言控制参数

当设备从下游接口接收到组播数据时，说明该网段中还存在其他的上游设备。设备从该接口发出Assert报文，参与竞选唯一上游。

## 前置任务

在调整断言控制参数之前，需完成以下任务：

**4.7.1 配置PIM-DM基本功能**

## 背景信息

当一个网段内有多个相连的PIM设备RPF检查通过向该网段转发组播数据时，则需要通过断言竞选来保证只有一个PIM设备向该网段转发组播数据。

在竞选中落败的PIM设备会抑制相应下游接口向该网段转发组播数据，但是这种竞选失败的状态只会保持一段时间，这段时间称为Assert报文的保持时间。超时后，落选的设备会重新恢复转发组播数据从而触发新一轮的竞选。

**说明**

Assert报文保持时间在全局PIM视图下和接口视图下都可配置，如果同时配置，接口视图上的配置生效。

## 缺省配置

表4-12列出了断言参数的缺省配置。

**表 4-12 断言参数的缺省配置**

| 参数 | 缺省值 |
| --- | --- |
| 保持Assert状态的时间 | 180s |

## 操作步骤

- 全局配置
  a. 执行命令**system-view**，进入系统视图。

b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

c. 执行命令**holdtime assert** *interval*，配置Assert报文的保持时间。

- 接口配置

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

c. 执行命令**pim holdtime assert** *interval*，配置Assert报文的保持时间。

**----结束**

## 检查配置结果

调整Assert控制参数成功后，可以通过命令查看PIM接口、PIM邻居信息和PIM路由表等信息。

- 执行命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]，查看接口上的PIM信息。
- 执行命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **neighbor** [ *neighbor-address* | **interface** *interface-type interface-number* | **verbose** ] *，查看PIM邻居信息。
- 使用以下命令查看PIM路由表：
  - 执行命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ]**routing-table** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm** ] * [ **outgoing-interface-number** [ *number* ] ]，查看PIM路由表详细信息。
  - 执行命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table brief** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } ] *，查看PIM路由表简要信息。

# 4.7.8 配置 PIM Silent

设备直连用户主机的接口上需要使能PIM协议，当恶意主机模拟PIM Hello报文，大量发送时，有可能导致设备瘫痪。为了避免这样的情况发生，可以将该接口设置为PIM Silent状态。

## 前置任务

在配置PIM Silent之前，需完成以下任务：

**4.7.1 配置PIM-DM基本功能**

## 背景信息

在接入层上，设备直连用户主机的接口上如果需要使能PIM协议，在该接口上可以建立PIM邻居，处理各类PIM协议报文。此配置同时存在着安全隐患：当恶意主机模拟发送PIM Hello报文时，有可能导致设备瘫痪。

为了避免这样的情况发生，可以将该接口设置为PIM Silent状态（即PIM消极状态）。当接口进入PIM消极状态后，禁止接收和转发任何PIM协议报文，删除该接口上的所有

PIM邻居以及PIM状态机，该接口作为静态DR立即生效。同时，该接口上的IGMP功能不受影响。

该功能仅适用于与用户主机网段直连的PIM设备接口，且该用户网段只与这一台PIM设备相连。

注意

配置了该功能后，接口将不再接收和转发任何PIM协议报文，即该接口配置的其他PIM功能将失效，请谨慎使用。

### 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**interface** *interface-type interface-number*，进入接口视图。

**步骤3** 执行命令**pim silent**，使能PIM Silent功能。

**----结束**

### 检查配置结果

配置PIM Silent成功后，可以通过如下命令查看PIM接口信息。

- 使用**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]查看接口上的PIM信息。

## 4.8 配置 PIM-SM（IPv4）

通过配置PIM协议，可以实现域内组播路由与数据转发。PIM-SM是稀疏模式的域内组播路由协议，适用于组成员分布相对分散、范围较广的大规模网络。

## 4.8.1 配置 ASM 模型的 PIM-SM

通过配置ASM模型的PIM-SM，可为用户主机提供任意源组播服务，加入同一组播组的用户主机都能收到任意源发往该组的组播数据。

### 前置任务

在配置ASM模型的PIM-SM之前，需配置单播路由协议，保证网络内单播路由畅通。

### 配置流程

配置ASM模型的PIM-SM必选步骤如下：

1. 使能PIM-SM
2. 配置RP

配置BSR管理域、配置SPT切换条件、调整源注册控制参数、调整C-RP参数、调整C-BSR参数为可选步骤，可根据实际需要进行选配。

### 4.8.1.1 使能 PIM-SM

## 背景信息

VPN实例或者公网实例上不能同时使能PIM-DM和PIM-SM。

建议将处于PIM-SM域内的所有接口都使能PIM-SM，以确保与相连PIM设备都能建立邻居关系。

如果接口上需要同时使能PIM-SM和IGMP，必须要先使能PIM-SM，再使能IGMP。

## 操作步骤

- 使能公网实例的PIM-SM
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**multicast routing-enable**，使能IP组播路由功能。
  c. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  d. 执行命令**pim sm**，使能PIM-SM功能。
- 使能VPN实例的PIM-SM

  使能VPN实例的PIM-SM之前，应该已经创建好VPN实例。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**ip vpn-instance** *vpn-instance-name*，进入VPN实例视图。
  c. 执行命令**multicast routing-enable**，使能IP组播路由功能。
  d. 执行命令**quit**，退回系统视图。
  e. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  f. 执行命令**ip binding vpn-instance** *vpn-instance-name*，将接口与VPN实例进行关联。
  g. 执行命令**pim sm**，使能PIM-SM功能。

**----结束**

### 4.8.1.2 配置 RP

## 背景信息

配置RP有手工静态RP配置和BSR动态收集扩散RP机制两种方式。手工方式静态配置RP，可以避免C-RP与BSR之间频繁的信息交互而占用带宽。通过BSR动态收集扩散RP机制动态选举，可以避免手工配置的繁琐；同时配置多台C-RP也可以保证组播数据转发的可靠性。

如果希望接收其他设备的Auto-RP宣告或发现报文，可以使能Auto-RP侦听功能。

**注意**

静态RP和动态RP可同时配置，此时静态RP由于默认优先级较低而被当作备份RP。但同时配置时需要确保设备间的RP信息一致，否则容易导致网络故障。

## 缺省配置

表4-13列出了C-BSR、C-RP部分参数的缺省配置。

**表 4-13** C-BSR、C-RP 部分参数的缺省配置

| 参数 | 缺省值 |
| --- | --- |
| C-BSR优先级 | 0 |
| C-BSR携带的哈希掩码长度 | 30 |
| BSR报文分片功能 | 未使能 |
| 静态RP组播组策略 | 没有组播组策略，即允许接收任意组地址的组播报文 |
| C-RP组播组策略 | 没有组播组策略，即允许接收任意组地址的组播报文 |
| C-RP优先级 | 0 |
| C-RP的宣告报文发送间隔 | 60s |
| C-RP的宣告报文保持时间 | 150s |

## 操作步骤

- 配置静态RP
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**static-rp** *rp-address* [ *basic-acl-number* | **acl-name** *acl-name* ] [ **preferred** ]，指定静态RP地址。

     指定**preferred**参数，表示静态RP优先级比动态RP高。

     **说明**

     在一个PIM-SM域内所有的PIM设备上都需指定相同的静态RP地址，保证静态RP正常运行。
- 配置动态RP
  a. 配置C-BSR
     i. 执行命令**system-view**，进入系统视图。
     ii. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
     iii. 执行命令**c-bsr** *interface-type interface-number* [ *hash-length* [ *priority* ] ]，配置C-BSR。

     建议在组播数据流量汇聚的设备上配置C-BSR。
     iv. （可选）执行命令**bsm semantic fragmentation**，使能BSR报文分片功能。

**说明**

使能BSR报文分片功能后，可以解决IP分片时分片信息丢失而导致所有分片不可用的问题。但是必须要保证所有设备都要使能，否则会导致未使能的设备接收到的RP信息不完整。

b. 配置C-RP

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

iii. 执行命令**c-rp** *interface-type interface-number* [ **group-policy** { *basic-acl-number* | **acl-name** *acl-name* } | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval* ] *，指定C-RP所在接口。

建议在组播数据流量汇聚的设备上配置C-RP。

c. （可选）配置BSR边界

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**interface** *interface-type interface-number*，进入接口视图。

iii. 执行命令**pim bsr-boundary**，配置BSR服务边界。

配置BSR边界后，BSR报文无法通过该边界，主要在划分PIM-SM域时使用。

建议在规划的PIM-SM域的边缘接口配置BSR服务边界。

- 使能Auto-RP侦听功能

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

c. 执行命令**auto-rp listening enable**，使能Auto-RP侦听功能。

**----结束**

### 4.8.1.3 （可选）配置 BSR 管理域

## 背景信息

为了更有效的管理PIM域，可将PIM域划分为多个BSR管理域和一个Global域。其中每个BSR管理域都维护一个BSR，服务于自己特定地址范围的组播组；Global域也维护一个BSR，为剩余不属于BSR管理域的组播组服务。一台设备只能加入一个管理域，因此各个管理域转发组播报文互不干涉；Global可以通过任意管理域内的设备进行报文转发。

BSR管理域可服务的最大组地址范围为239.0.0.0～239.255.255.255。该段地址可重复使用，相当于每个BSR管理域的私有组地址。

## 操作步骤

**步骤1** 在PIM域内所有设备上使能BSR管理域功能

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
3. 执行命令**c-bsr admin-scope**，使能BSR管理域功能。

**步骤2** 在每个BSR管理域的边缘接口上配置边界

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**interface** *interface-type interface-number*，进入接口视图。
3. 执行命令**multicast boundary** *group-address* { *mask* | *mask-length* }，配置BSR管理域边界。

   限定了组地址范围后，该范围内的组播报文将无法通过此接口进行转发。

**步骤3** 在每个BSR管理域的C-BSR上配置服务的组地址范围

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
3. 执行命令**c-bsr group** *group-address* { *mask* | *mask-length* } [ **hash-length** *hash-length* | **priority** *priority* ] *，配置C-BSR服务的组地址范围。

**步骤4** 配置Global域的C-BSR

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
3. 执行命令**c-bsr global** [ **hash-length** *hash-length* | **priority** *priority* ] *，配置Global域的C-BSR。

**----结束**

### 4.8.1.4 （可选）配置 SPT 切换条件

## 背景信息

当组播流量变大时，RP上的负担增大，容易引发故障，此时可通过组成员端DR发起到源的SPT切换来减轻RP的压力。

缺省情况下，组成员端DR在接收到第一份组播数据报文后都会向源方向发起SPT切换。如果希望通过设置组播速率阈值来触发SPT切换或者不发起SPT切换，可在组成员端DR配置此功能。

## 缺省配置

表4-14列出了SPT切换条件相关的缺省配置。

**表 4-14** SPT 切换条件相关的缺省配置

| 参数 | 缺省值 |
| --- | --- |
| SPT切换条件的组播组策略 | 没有组播组策略，即SPT切换条件会应用于所有组播组 |
| 检查组播数据转发速率的时间间隔 | 15s |

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

**步骤3** 执行命令**spt-switch-threshold** { *traffic-rate* | **infinity** } [ **group-policy** { *basic-acl-number* | **acl-name** *acl-name* } [ **order** *order-value* ] ]，配置SPT切换条件。

*traffic-rate*表示允许执行切换的速率阈值；**infinity**表示永远不发起SPT切换。

**步骤4** 执行命令**timer spt-switch** *interval*，配置检查组播数据转发速率的时间间隔。

**----结束**

### 4.8.1.5 （可选）调整注册控制参数

## 背景信息

源端DR在收到组播源发送来的组播数据后，会将其封装在注册报文中转发给RP。因此注册报文控制参数主要在RP和源端DR两个位置进行调整。

在源端DR上可进行如下调整：

- 配置注册Register抑制时间。源端DR在收到RP发来的注册停止Register-stop报文后，在注册抑制时间内，会停止向RP发送注册报文。超时后，如果源端DR没有收到后续的注册停止报文，则恢复相应注册报文的转发。
- 配置发送空注册报文时间间隔。如果注册抑制时间过大或过小，都会影响组播数据的正常转发。通过在抑制期间发空注册报文，可以改善这种影响。
- 配置仅根据注册报文头来计算校验和，可减少计算校验和的时间，提高注册报文封装组播数据的效率。
- 配置注册报文的源地址。如果当前源DR向RP发送的注册报文的源地址对于RP来说不是网络中唯一的IP地址，或者RP上配置了过滤策略将该地址已过滤掉，RP都不会接收到注册报文。此时，通过重新指定合理的源IP地址，可解决此问题。

在RP上可进行如下调整：

- 配置过滤注册报文的规则，可限定注册报文的地址范围，提高网络安全性。

## 缺省配置

表4-15列出了注册控制参数的缺省配置。

**表 4-15 注册控制参数的缺省配置**

| 参数 | 缺省值 |
| --- | --- |
| 注册报文过滤策略 | 无过滤策略，即允许接收任意组地址的注册报文 |
| 注册报文校验方式 | RP根据整个注册报文来计算校验和 |
| 注册抑制时间 | 60s |
| 发送空注册报文时间间隔 | 5s |

## 操作步骤

- 在源端DR上配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**register-suppression-timeout** *interval*，配置保持注册抑制状态的超时时间。
  d. 执行命令**probe-interval** *interval*，配置发送空注册报文的时间间隔。

     **说明**

     **probe-interval**的值必须小于**register-suppression-timeout**值的二分之一。
  e. 执行命令**register-header-checksum**，配置根据注册报文头信息计算校验和，未通过校验的Register注册报文将被丢弃。
  f. 执行命令**register-source** *interface-type interface-number*，指定源DR发送注册报文的源地址。

     在指定源DR发送注册报文的源地址时，建议使用源DR上Loopback接口的IP地址。
- 在RP上配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**register-policy** { *advanced-acl-number* | **acl-name** *acl-name* }，配置过滤注册报文的规则。

**----结束**

### 4.8.1.6 （可选）调整 C-RP 控制参数

## 背景信息

在设备上配置了C-RP后，C-RP会周期性地向BSR发送Advertisement报文（以下称宣告报文），报文携带C-RP优先级、宣告报文的保持时间。BSR在收到该报文后，启动C-RP超时定时器，时间设为宣告报文的保持时间。在超时前，BSR将宣告报文中携带的C-RP信息汇总成RP-Set信息，封装在自举报文中向PIM域中的所有PIM设备发送。超时后，如果BSR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。所以C-RP发送宣告报文时间间隔必须要小于宣告报文的保持时间。

C-RP发送宣告报文时间间隔、C-RP优先级、宣告报文的保持时间都可进行手工配置。有时候为了防止非法C-RP欺骗，还可在BSR上设置合法的C-RP地址范围，只接收该地址范围内C-RP的宣告报文。

**说明**

有关宣告报文携带的参数的缺省值，可参见**4.8.1.2 配置RP**。

## 操作步骤

- 在C-RP上配置宣告报文携带的参数。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**c-rp priority** *priority*，配置C-RP优先级。

d. 执行命令**c-rp advertisement-interval** *interval*，配置C-RP发送宣告报文的间隔时间。

e. 执行命令**c-rp holdtime** *interval*，配置保持来自C-RP的宣告报文的时间。

- 在BSR上限定合法的C-RP地址范围。

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

c. 执行命令**crp-policy** { *advanced-acl-number* | **acl-name** *acl-name* }，限定合法的C-RP地址范围及其服务的组播组地址范围。

**----结束**

## 4.8.1.7 （可选）调整 C-BSR 控制参数

## 背景信息

BSR由C-BSR之间自动选举产生。选举开始时，每个C-BSR都认为自己是本PIM域的BSR，向域内所有PIM设备发送Bootstrap报文（以下称自举报文）。C-BSR在接收到其他C-BSR发来的自举报文后，首先比较二者的优先级，优先级较高者获胜；若优先级相同，则再比较二者IP地址，IP地址较大者获胜。获胜者将成为域内的BSR，它会将自己的IP地址和RP-Set信息封装在自举报文中向域内发送。自举报文还携带哈希掩码信息，在C-RP竞选中如果要进行哈希计算时需要。

BSR周期性地发送自举报文，其他的C-BSR收到该报文后会启动超时定时器，时间设为自举报文的保持时间；超时后如果没有接收到BSR发来的自举报文，C-BSR之间会触发新一轮的BSR选举过程。所以BSR发送自举报文的时间间隔必须要小于自举报文的保持时间。

C-BSR优先级、BSR哈希掩码、BSR发送自举报文时间间隔、自举报文的保持时间都可进行手工配置。有时候为了防止非法BSR欺骗，还可在PIM设备上设置合法的BSR地址范围，只接收该地址范围内BSR的自举报文。

## 缺省配置

表4-16列出了C-BSR部分参数的缺省配置。

**表 4-16** C-BSR 部分参数的缺省配置

| 参数 | 缺省值 |
| --- | --- |
| 发送自举报文的时间间隔 | 60s |
| 自举报文的保持时间 | 130s |

**说明**

有关C-BSR其他参数的缺省值，可参见**4.8.1.2 配置RP**。

## 操作步骤

- 在C-BSR上配置自举报文携带的参数。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**c-bsr priority** *priority*，配置C-BSR的优先级。
  d. 执行命令**c-bsr hash-length** *priority*，配置BSR的哈希掩码。
  e. 执行命令**c-bsr interval** *interval*，配置BSR发送自举报文的间隔时间。
  f. 执行命令**c-bsr holdtime** *interval*，配置保持来自BSR的自举报文时间。
- 在PIM设备上限定合法的BSR地址范围。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**bsr-policy** { *basic-acl-number* | **acl-name** *acl-name* }，限定合法BSR地址范围。

**----结束**

## 4.8.1.8 检查配置 ASM 模型的 PIM-SM 的结果

## 前提条件

配置ASM的PIM-SM完成后，可以通过命令查看BSR、RP、PIM接口、PIM邻居和PIM路由表等信息。

## 操作步骤

- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **bsr-info**，查看BSR的信息。
- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **rp-info** [ *group-address* ]，查看RP信息。
- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]，查看接口上的PIM信息。
- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **neighbor** [ *neighbor-address* | **interface** *interface-type interface-number* | **verbose** ] *，查看PIM邻居信息。
- 使用以下命令查看PIM路由表：
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm** ] * [ **outgoing-interface-number** [ *number* ] ]
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table brief** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } ] *

**----结束**

# 4.8.2 配置 SSM 模型的 PIM-SM

通过配置SSM模型的PIM-SM，可以为用户主机提供指定组播源服务，加入同一组播组的用户主机可以按各自需要只接收指定源的组播数据。

## 前置任务

在配置SSM模型的PIM-SM之前，需配置单播路由协议，保证网络内单播路由畅通。

## 配置流程

使能PIM-SM为必选步骤。配置SSM组策略为可选步骤，主要用来控制SSM组地址范围。

### 4.8.2.1 使能 PIM-SM

## 背景信息

VPN实例或者公网实例上不能同时使能PIM-DM和PIM-SM。

建议将处于PIM-SM域内的所有接口都使能PIM-SM，以确保与相连PIM设备都能建立邻居关系。

如果接口上需要同时使能PIM-SM和IGMP，必须要先使能PIM-SM，再使能IGMP。

## 操作步骤

- 使能公网实例的PIM-SM
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**multicast routing-enable**，使能IP组播路由功能。
  c. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  d. 执行命令**pim sm**，使能PIM-SM功能。
- 使能VPN实例的PIM-SM

  使能VPN实例的PIM-SM之前，应该已经创建好VPN实例。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**ip vpn-instance** *vpn-instance-name*，进入VPN实例视图。
  c. 执行命令**multicast routing-enable**，使能IP组播路由功能。
  d. 执行命令**quit**，退回系统视图。
  e. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  f. 执行命令**ip binding vpn-instance** *vpn-instance-name*，将接口与VPN实例进行关联。
  g. 执行命令**pim sm**，使能PIM-SM功能。

**----结束**

### 4.8.2.2 （可选）配置 SSM 组策略

## 背景信息

SSM的组地址缺省范围是232.0.0.0/8。有时候希望限制SSM组地址范围，保证组播网络安全；或者SSM组地址不够用，需要扩展SSM组地址范围。此时，可通过配置SSM组策略，控制SSM的组地址范围。

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

**步骤3** 执行命令**ssm-policy** { *basic-acl-number* | **acl-name** *acl-name* }，配置SSM组地址范围。

**说明**

确保网络内所有PIM设备上配置的SSM组地址范围都一致。

**----结束**

### 4.8.2.3 检查配置 SSM 模型的 PIM-SM 的结果

## 前提条件

配置SSM的PIM-SM完成后，可以通过命令查看PIM接口、PIM邻居和PIM路由表等信息。

## 操作步骤

- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]，查看接口上的PIM信息。
- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **neighbor** [ *neighbor-address* | **interface** *interface-type interface-number* | **verbose** ] *，查看PIM邻居信息。
- 使用以下命令查看PIM路由表：
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm** ] * [ **outgoing-interface-number** [ *number* ] ]
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table brief** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } ] *

**----结束**

# 4.8.3 调整组播源控制参数

通过过滤组播源地址，以及对组播源生存时间进行控制，可以提高数据安全性、控制网络流量。

## 前置任务

在调整组播源控制参数之前，需完成以下任务：

- 配置单播路由协议，保证网络内单播路由畅通。
- 使能PIM-SM。

## 背景信息

当PIM设备在接收到源S发出的组播报文后，就会启动该（S，G）表项的定时器，时间设为源生存时间。如果超时前接收到源S后续发来的报文，则重置定时器；如果超时后没有接收到源S后续发来的报文，则认为（S，G）表项失效，将其删除。源生存时间可以手动配置。

如果希望控制组播流量或者保证接收数据的安全性，还可在PIM设备上配置源地址过滤策略，只接收该策略允许范围内的组播数据。

## 缺省配置

表4-17列出了组播源控制参数的缺省配置。

**表 4-17 组播源控制参数的缺省配置**

| 参数 | 缺省值 |
| --- | --- |
| 组播源生存时间 | 210s |
| 源地址过滤策略 | 没有过滤策略，即接收任何组播源发来的组播数据 |

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

**步骤3** 执行命令**source-lifetime** *interval*，配置组播源生存时间。

**步骤4** 执行命令**source-policy** { *acl-number* | **acl-name** *acl-name* }，配置源地址过滤策略。

- 如果配置的是基本ACL，通过与**rule**中的**source**参数配合，只转发源地址属于过滤规则允许范围的组播报文。
- 如果配置的是高级ACL，通过与**rule**中的**source**和**destination**参数配合，只转发源地址和组地址都属于过滤规则允许范围内的组播报文。
- 执行此命令后，如果指定ACL没有配置过滤规则，则不转发任何源地址发送的组播报文。
- 如果当前PIM表项是通过学习静态配置指定（S，G）的IGMP组信息而生成的，执行此命令后，不过滤对应PIM表项的组播报文。

**----结束**

## 检查配置结果

调整组播源控制参数成功后，可以通过命令查看PIM路由表中的表项是否符合要求。

使用以下命令查看PIM路由表：

- **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm** ] * [ **outgoing-interface-number** [ *number* ] ]
- **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table brief** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } ] *

## 4.8.4 调整邻居控制参数

PIM设备之间通过交互Hello报文建立邻居关系。

### 前置任务

在调整邻居控制参数之前，需完成以下任务：

- 配置单播路由协议，保证网络内单播路由畅通。
- 使能PIM-SM。

### 配置流程

Hello报文的时间控制参数、邻居跟踪功能、邻居过滤策略配置时并无先后顺序，可根据实际需要进行调整。

#### 4.8.4.1 调整 Hello 报文的时间控制参数

### 背景信息

PIM设备通过周期性地发送Hello报文来维护PIM邻居关系。当PIM设备收到邻居发来Hello报文后，会启动定时器，时间设为该Hello报文的保持时间。如果超时后没有收到邻居发来的Hello报文，则认为该邻居失效或者不可达。因此，PIM设备发送Hello报文的时间间隔必须要小于Hello报文的保持时间。

为了避免多个PIM设备同时发送Hello报文而导致冲突，当PIM设备接收到Hello报文时，将延迟一段时间再发送Hello报文。该段时间的值为一个随机值，并且小于“触发Hello报文的最大延迟”。

**说明**

发送Hello报文的时间间隔、Hello报文的保持时间在全局PIM视图下和接口视图下都可配置。如果同时配置，接口视图上的配置生效。

触发Hello报文的最大延迟时间只能在接口上配置。

### 缺省配置

表4-18列出了Hello报文时间参数的缺省配置。

**表 4-18** Hello 报文时间参数的缺省配置

| 参数 | 缺省值 |
| --- | --- |
| 发送Hello报文的时间间隔 | 30s |
| Hello报文的保持时间 | 105s |
| 触发Hello报文的最大延迟时间 | 5s |

## 操作步骤

- 全局配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**timer hello** *interval*，配置发送Hello报文的时间间隔。
  d. 执行命令**hello-option holdtime** *interval*，配置Hello报文的保持时间。
- 接口配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**pim timer hello** *interval*，配置发送Hello报文的时间间隔。
  d. 执行命令**pim hello-option holdtime** *interval*，配置Hello报文的保持时间。
  e. 执行命令**pim triggered-hello-delay** *interval*，配置触发Hello报文的最大延迟。

**----结束**

## 4.8.4.2 配置跟踪下游邻居功能

## 背景信息

设备发送Hello报文时，会生成一个Generation ID携带在该报文中。一般Generation ID不会改变，只有设备状态改变，此时Generation ID重新生成才会改变。这时邻居设备在收到Hello报文后，发现Generation ID改变，会立即向该设备发送加入报文以刷新邻居关系。正常情况下，如果共享网段内有多台设备都准备向同一上游设备发送加入请求，会采用侦听机制来抑制这种相同加入报文的数目，即一台设备在侦听到其他设备的加入报文后，将不会再向该上游PIM邻居发送加入报文。所以，这时候因Generation ID改变的上游邻居无法刷新与每台下游的邻居关系。

配置了跟踪下游邻居跟踪功能后，设备在侦听到其他设备发送的加入报文时，将不会抑制向相同的上游PIM邻居发送加入报文。

**说明**

跟踪下游邻居功能在全局PIM视图下和接口视图下都可配置。如果同时配置，接口视图上的配置生效。

配置跟踪下游邻居功能时，必须保证共享网段中的所有设备都使能该功能。

## 操作步骤

- 全局配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**hello-option neighbor-tracking**，使能跟踪下游邻居功能。
- 接口配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**pim hello-option neighbor-tracking**，使能跟踪下游邻居功能。

**----结束**

### 4.8.4.3 配置邻居过滤策略

## 背景信息

路由器支持不同的邻居过滤策略，来保证PIM域的安全和畅通：

- 限定合法的邻居地址范围，防止非法邻居入侵。
- 拒绝接收无Generation ID的Hello报文，保证路由器相连的都是正常工作的PIM邻居。
- 使能邻居检查功能，丢弃非邻居发来的Join/Prune报文和Assert报文；或者不向非邻居发送Join/Prune报文和Assert报文。

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**interface** *interface-type interface-number*，进入接口视图。

**步骤3** 执行命令**pim neighbor-policy** { *basic-acl-number* | **acl-name** *acl-name* }，配置合法的邻居地址范围。

- 设备上配置了合法的邻居地址范围后，如果之前与其建立好邻居关系的PIM设备不在其合法地址范围内，后续将不会再收到邻居设备的Hello报文。邻居关系也会因Hello报文的保持时间超时而解除。

**步骤4** 执行命令**pim require-genid**，配置只接收包含Generation ID的Hello报文。

**步骤5** 执行命令**quit**，退出接口视图。

**步骤6** 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

**步骤7** 执行命令**neighbor-check** { **receive** | **send** }，配置邻居检查功能。

**----结束**

### 4.8.4.4 检查配置调整邻居控制参数的结果

## 前提条件

调整邻居控制参数成功后，可以通过命令查看PIM接口和PIM邻居是否符合要求。

## 操作步骤

- 使用**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]命令查看接口上的PIM信息。
- 使用**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **neighbor** [ *neighbor-address* | **interface** *interface-type interface-number* | **verbose** ] *命令查看PIM邻居信息。

----结束

# 4.8.5 调整 DR 竞选控制参数

设备之间通过交互Hello报文选举DR，主要负责源端或者组成员端的协议报文发送的工作。

## 前置任务

在调整DR竞选控制参数之前，需完成以下任务：

- 配置单播路由协议，保证网络内单播路由畅通。
- 使能PIM-SM。

## 配置流程

DR竞选优先级、DR切换延迟功能配置时并无先后顺序，用户可根据实际需要进行调整。

### 4.8.5.1 配置 DR 优先级

## 背景信息

在组播源或组成员所在的共享网段，通常同时连接着多台PIM设备。为了争取该网段唯一的组播报文转发权，PIM设备之间就需要通过交互Hello报文进行DR竞选。竞选时，首先比较Hello报文中携带的DR优先级，优先级较高者获胜（优先级数值越大，表示优先级越高）；如果DR优先级相同或该网段存在至少一台PIM设备不支持在Hello报文中携带DR优先级，则IP地址较大者获胜。

**说明**

DR优先级在全局PIM视图下和接口视图下都可配置，如果同时配置，接口视图上的配置生效。

## 缺省配置

表4-19列出了DR优先级的缺省配置。

**表 4-19** DR 优先级的缺省配置

| 参数 | 缺省值 |
| --- | --- |
| DR优先级 | 1 |

## 操作步骤

- 全局配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**hello-option dr-priority** *priority*，配置竞选DR的优先级。
- 接口配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**pim hello-option dr-priority** *priority*，配置竞选DR的优先级。

**----结束**

### 4.8.5.2 配置 DR 切换延迟

## 背景信息

有时候由于某些原因，当前共享网段的DR变成非DR，原有向该网段的转发数据的组播表项会被立即删除，这可能会导致短时间内组播数据的断流。此时，可以配置DR切换延迟，并指定延迟时间，原有表项仍然有效直到延迟时间超时。

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**interface** *interface-type interface-number*，进入接口视图。

**步骤3** 执行命令**pim timer dr-switch-delay** *interval*，配置DR切换延迟，并指定延迟时间。

缺省情况下，当出接口由DR变为非DR时，出接口立即停止转发数据。

**----结束**

### 4.8.5.3 检查配置调整 DR 竞选控制参数的结果

## 前提条件

调整DR竞选控制参数成功后，可以通过命令查看PIM接口和PIM邻居是否符合要求。

## 操作步骤

- 使用**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]命令查看接口上的PIM信息。
- 使用**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **neighbor** [ *neighbor-address* | **interface** *interface-type interface-number* | **verbose** ] *命令查看PIM邻居信息。

**----结束**

# 4.8.6 调整加入和剪枝控制参数

设备向上游发送Join信息请求转发组播数据，发送Prune信息请求停止转发组播数据。可以根据实际需要调整转发控制参数，若无特殊需要，推荐使用缺省值。

## 前置任务

在调整加入和剪枝控制参数之前，需完成以下任务：

- 配置单播路由协议，保证网络内单播路由畅通。
- 使能PIM-SM。

## 配置流程

Join/Prune报文的时间控制参数、Join/Prune报文的信息携带能力、剪枝延迟时间、加入信息过滤策略配置时并无先后顺序，用户可根据实际需要进行调整。

## 4.8.6.1 调整 Join/Prune 报文的时间控制参数

## 背景信息

PIM设备通过向上游发送Join信息请求转发组播数据，发送Prune信息请求停止转发组播数据。实际上，Join信息和Prune信息都被封装在了Join/Prune报文中，PIM设备会周期性的将Join/Prune报文发送给上游设备来更新转发状态。上游设备在收到Join/Prune报文，就会启动定时器，时间设为Join/Prune报文自身携带的保持时间。超时后，如果没有收到下游后续发来的Join/Prune报文：

- 若未收到的Join/Prune报文携带有加入某组播组信息，则抑制相应组播组下游接口的转发；
- 若未收到的Join/Prune报文携带有针对某组播组的剪枝信息，则恢复相应组播组下游接口的转发。

因此Join/Prune报文的发送间隔必须要小于Join/Prune报文的保持时间。

**说明**

发送Join/Prune报文的时间间隔、Join/Prune报文的保持时间在全局PIM视图下和接口视图下都可配置，如果同时配置，接口视图上的配置生效。

## 缺省配置

表4-20列出了Join/Prune报文时间参数的缺省配置。

**表 4-20** Join/Prune 报文时间参数的缺省配置

| 参数 | 缺省值 |
| --- | --- |
| 发送Join/Prune报文的时间间隔 | 60s |
| Join/Prune报文的保持时间 | 210s |

## 操作步骤

- 全局配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**timer join-prune** *interval*，配置发送Join/Prune报文的时间间隔。
  d. 执行命令**holdtime join-prune** *interval*，配置Join/Prune报文的保持时间。
- 接口配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**pim timer join-prune** *interval*，配置发送Join/Prune报文的时间间隔。
  d. 执行命令**pim holdtime join-prune** *interval*，配置Join/Prune报文的保持时间。

**----结束**

## 4.8.6.2 调整 Join/Prune 报文的信息携带能力

## 背景信息

路由器支持通过配置Join/Prune报文长度、包含表项数目、发送方式，来调整PIM设备向上游发送加入和剪枝信息的信息量：

- 当PIM邻居设备性能比较差，处理单个Join/Prune报文耗时比较长，可以通过调整发送的Join/Prune报文长度来控制发送Join/Prune报文携带的(S, G)表项数量，来降低PIM邻居设备的压力。
- 当PIM邻居设备Join/Prune报文处理吞吐量比较小时，可以通过调整周期性报文发送队列长度，控制每次发给PIM邻居设备的(S, G)表项数量，采取小量多批次方式发送Join/Prune报文，从而避免PIM邻居设备来不及处理就将报文丢弃，引起路由振荡。
- 缺省情况下，为了提高发送效率，Join/Prune报文都是打包向上游发送。如果不希望Join/Prune报文打包发送，可去使能此功能。

## 缺省配置

表4-21列出了Join/Prune报文部分参数的缺省配置。

**表 4-21** Join/Prune 报文部分参数的缺省配置

| 参数 | 缺省值 |
| --- | --- |
| Join/Prune报文长度 | 8100字节 |
| Join/Prune报文包含的表项数目 | 1020个 |
| Join/Prune报文的发送方式 | 打包发送 |

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

**步骤3** 执行命令**join-prune max-packet-length** *packet-length*，配置PIM-SM发送的Join/Prune报文的最大长度。

**步骤4** 执行命令**join-prune periodic-messages queue-size** *queue-size*，配置PIM-SM每秒发送Join/Prune报文中包含的表项数目。

**步骤5** 执行命令**join-prune triggered-message-cache disable**，去使能实时触发的Join/Prune报文打包功能。

**----结束**

## 4.8.6.3 调整剪枝延迟时间

## 背景信息

在剪枝过程中，从收到下游设备发来的剪枝信息到继续向上游设备发送剪枝信息都会有延迟时间，这段时间称为LAN-Delay。PIM设备在向上游发完剪枝信息后，也不会立即将相应下游接口剪掉，还会保持一段时间向下游转发。如果下游又有组播需求，必须要在这段时间内发送加入请求以否决这个剪枝动作。这段否决剪枝的时间称为Override-Interval。所以，实际上PIM设备从收到剪枝信息到完成剪枝动作总共延迟了LAN-Delay＋Override-Interval段时间。

**说明**

LAN-Delay、Override-Interval在全局PIM视图下和接口视图下都可配置，如果同时配置，接口视图上的配置生效。

## 缺省配置

表4-22列出了剪枝延迟时间参数的缺省配置。

**表 4-22 剪枝延迟时间参数的缺省配置**

| 参数 | 缺省值 |
| --- | --- |
| LAN-Delay | 500ms |
| Override-Interval | 2500ms |

## 操作步骤

- 全局配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。
  c. 执行命令**hello-option lan-delay** *interval*，配置共享网络内传递报文的延迟时间。

d. 执行命令**hello-option override-interval** *interval*，配置否决剪枝的时间间隔。

- 接口配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**pim hello-option lan-delay** *interval*，配置共享网络内传递报文的延迟时间。
  d. 执行命令**pim hello-option override-interval** *interval*，配置否决剪枝的时间间隔。

**----结束**

### 4.8.6.4 配置 Join 信息的过滤策略

## 背景信息

有时候为了防止非法用户的加入，还可配置Join信息过滤策略，指定Join/Prune报文中Join信息的合法源地址范围。

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**interface** *interface-type interface-number*，进入接口视图。

**步骤3** 执行命令**pim join-policy** { **asm** { *basic-acl-number* | **acl-name** *acl-name* } | **ssm** { *advanced-acl-number* | **acl-name** *acl-name* } | *advanced-acl-number* | **acl-name** *acl-name* }，配置Join信息过滤策略，限定Join信息的合法源地址范围。

**----结束**

### 4.8.6.5 检查配置调整加入和剪枝控制参数的结果

## 前提条件

调整加入和剪枝控制参数成功后，可以通过命令查看PIM接口、PIM控制消息统计数和PIM路由表等信息。

## 操作步骤

- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]，查看接口上的PIM信息。
- 使用以下命令查看PIM发送和接收的PIM控制报文的数目信息：
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **control-message counters message-type** { **probe** | **register** | **register-stop** | **crp** }
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **control-message counters** [ **message-type** { **assert** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** | **bsr** } | **interface** *interface-type interface-number* ] *
- 使用以下命令查看PIM路由表：
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address*

[ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm** ] * [ **outgoing-interface-number** [ *number* ] ]

- **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table brief** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } ] *

----结束

## 4.8.7 调整断言控制参数

当设备从下游接口接收到组播数据时，说明该网段中还存在其他的上游设备。设备从该接口发出Assert报文，参与竞选唯一上游。

### 前置任务

在调整断言控制参数之前，需完成以下任务：

- 配置单播路由协议，保证网络内单播路由畅通。
- 使能PIM-SM。

### 背景信息

当一个网段内有多个相连的PIM设备均通过了RPF检查从而可以向该网段转发组播数据时，需要通过断言竞选来保证只有一个PIM设备向该网段转发组播数据。

在竞选中落败的PIM设备会抑制相应下游接口向该网段转发组播数据，但是这种竞选失败的状态只会保持一段时间。这段时间称为Assert报文的保持时间。超时后，落选的设备会重新恢复转发组播数据从而触发新一轮的竞选。

**说明**

Assert报文保持时间在全局PIM视图下和接口视图下都可配置，如果同时配置，接口视图上的配置生效。

### 缺省配置

表4-23列出了断言参数的缺省配置。

**表 4-23 断言参数的缺省配置**

| 参数 | 缺省值 |
| --- | --- |
| 保持Assert状态的时间 | 180s |

### 操作步骤

- 全局配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

c. 执行命令**holdtime assert** *interval*，配置Assert报文的保持时间。

- 接口配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**pim holdtime assert** *interval*，配置Assert报文的保持时间。

**----结束**

### 检查配置结果

调整Assert控制参数成功后，可以通过命令查看PIM接口、PIM邻居信息和PIM路由表等信息。

- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]查看接口上的PIM信息。
- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **neighbor** [ *neighbor-address* | **interface** *interface-type interface-number* | **verbose** ] *查看PIM邻居信息。
- 使用以下命令查看PIM路由表：
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm** ] * [ **outgoing-interface-number** [ *number* ] ]
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table brief** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } ] *

## 4.8.8 配置基于 PIM 的 Anycast RP

Anycast RP是指在同一个PIM-SM域内设置多个具有相同地址的RP，并在RP之间建立对等体关系，从而实现组播源就近注册和接收者就近加入。既可以缓解单个RP的负担，也实现了RP备份，优化了转发路径。

### 背景信息

目前支持两种方案实现PIM-SM域内Anycast RP：基于MSDP协议的Anycast RP和基于PIM协议的Anycast RP。在进行IPv4网络部署时，可以采用其中一种方案，不推荐两种方案同时使用。

### 前置任务

在配置基于PIM协议的Anycast RP之前，需完成以下任务：

- 配置单播路由协议，实现网络层互通
- **4.8.1 配置ASM模型的PIM-SM**

## 配置流程

根据以下描述内容的顺序配置Anycast RP。

### 4.8.8.1 配置全局 Anycast RP

## 背景信息

网络中可采用静态或动态RP，推荐将RP配置在Loopback接口上。请在有待建立Anycast RP的多台路由器上分别配置相同RP地址。

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

**步骤3** 执行命令**anycast-rp** *rp-address*，配置Anycast RP。

请将Anycast RP地址配置为与网络中的RP地址相同。

**----结束**

### 4.8.8.2 配置 Anycast RP 本地地址

## 背景信息

配置为Anycast RP的多台设备对外呈现相同的逻辑地址，使PIM-SM域内的RP唯一。但这些设备之间在进行通讯过程中需要区分彼此，因此不能使用配置的Anycast RP地址，而需要配置Anycast RP本地地址和Anycast RP对等体。

配置Anycast RP本地地址后，设备向Anycast RP对等体转发注册报文时，将源地址转换为配置的Anycast RP本地地址。

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

**步骤3** 执行命令**anycast-rp** *rp-address*，进入Anycast-RP视图。

**步骤4** 执行命令**local-address** *local-address*，配置Anycast RP本地地址。

**说明**

推荐使用Loopback接口地址作为Anycast RP本地地址。

Anycast RP本地地址不能与Anycast RP地址相同。

**----结束**

### 4.8.8.3 配置 Anycast RP 对等体

## 背景信息

配置为Anycast RP的多台设备对外呈现相同的逻辑地址，使PIM-SM域内的RP唯一。但这些设备之间在进行通讯过程中需要区分彼此，因此不能使用配置的Anycast RP地址，而需要配置Anycast RP本地地址和Anycast RP对等体。

配置Anycast RP对等体后，设备向Anycast RP对等体转发注册报文时，将目的地址转换为配置的Anycast RP对等体地址。

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

**步骤3** 执行命令**anycast-rp** *rp-address*，进入Anycast-RP视图。

**步骤4** 执行命令**peer** *peer-address* [ **fwd-msdp-sa** [ *acl-number* | **acl-name** *acl-name* ] ]，配置Anycast RP对等体。

在同一PIM-SM域内，配置的Anycast RP之间逻辑上需要配置为全连接结构，即任意两个Anycast RP之间需要配置为Anycast RP对等体。

**----结束**

### 4.8.8.4 检查配置基于 PIM 的 Anycast RP 的结果

## 背景信息

基于PIM协议的Anycast RP配置完成后，可以通过命令查看Anycast RP是否已配置成功。

## 操作步骤

- 使用**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **rp-info**命令查看RP信息。
- 使用以下命令查看PIM路由表：
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm** ] * [ **outgoing-interface-number** [ *number* ] ]
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table brief** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } ] *

**----结束**

# 4.8.9 配置 PIM GR

PIM-SM网络中，在具有双主控板的设备上配置PIM GR功能，设备进行主备倒换时可以保持用户组播流量的正常转发。

## 前置任务

在配置PIM GR之前，需完成以下任务：

- 配置单播路由协议，保证网络内单播路由畅通。
- 使能PIM-SM。

## 背景信息

**说明**

仅AR3200系列支持PIM GR。

在组播的应用中，组播设备有时需要进行主备倒换，比如设备升级、主控板发生故障等。在主用主控板和备用主控板进行倒换后，新主控板删除接口板的组播转发表项，重新学习PIM路由表及组播转发表。该过程中用户的组播流量会断流。

配置了PIM GR功能后，在发生主备倒换时，组播设备的主用主控板向备用主控板备份PIM路由表项以及需要向上游发送的Join/Prune的相关信息，接口板保留转发表项。主备倒换完成后，该组播设备就可以主动快速的向上游发送Join信息，维持上游的加入状态。同时，PIM协议向所有使能PIM-SM的组播设备发送携带新Generation ID的Hello报文，当下游组播设备发现其邻居的Generation ID发生了变化，便向邻居发送Join/Prune报文以帮助其重新建立路由表项，从而保证转发平面组播数据的不间断转发。

若网络中使用动态RP，当网络中的DR收到Generation ID改变的Hello报文后，会向发生主备倒换的组播设备单播发送Bootstrap报文（以下称自举报文），组播设备从该自举报文中学习并恢复RP信息。若组播设备未能从自举报文中学习到网络中的RP信息，则从下游发送的Join/Prune报文中获取RP信息，重新创建组播路由表。

## 缺省配置

表4-24列出了PIM GR参数的缺省配置。

**表 4-24** PIM GR 参数的缺省配置

| 参数 | 缺省值 |
| --- | --- |
| PIM GR周期 | 120s |

## 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**pim** [ **vpn-instance** *vpn-instance-name* ]，进入PIM视图。

**步骤3** 执行命令**graceful-restart**，使能PIM GR功能。

缺省情况下，没有使能PIM GR功能。

**步骤4** （可选）执行命令**graceful-restart period** *period*，配置PIM GR的最小周期。

缺省情况下，PIM GR最小周期为120秒。

**----结束**

### 检查配置结果

配置PIM GR成功后，可以通过以下命令查看PIM路由表中的表项是否符合要求。

- **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm** ] * [ **outgoing-interface-number** [ *number* ] ]
- **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table brief** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } ] *

## 4.8.10 配置 PIM BFD

当BFD检测到对端故障以后上报PIM模块，PIM模块立即触发新一轮的DR竞选过程，而不是等到邻居关系超时，这将很大程度上缩小组播数据传输的中断时间，提高组播网络的可靠性。

### 前置任务

在配置PIM-BFD之前，需完成以下任务：

- 配置单播路由协议，保证网络内单播路由畅通。
- 执行**bfd**命令全局使能BFD。
- 使能PIM-SM。

### 背景信息

在PIM协议运行过程中，PIM邻居间链路状态的变化会触发某些工作机制（如DR选举、Assert Winner选举）重新进行。比如共享网段上的当前DR发生故障，其他PIM邻居会等到邻居关系超时才触发新一轮的DR竞选过程，导致组播数据传输中断，中断的时间将不小于邻居关系的超时时间，通常是秒级。

PIM BFD能够在毫秒级内检测共享网段内的链路状态，快速响应PIM邻居故障。如果配置了PIM BFD功能的接口在检测周期内没有收到当前DR发送的BFD检测报文，则认为当前DR发生故障，BFD快速把会话状态通告给路由管理模块（RM），再由RM通告给PIM。PIM模块触发新一轮的DR竞选过程，而不是等到邻居关系超时，从而减少组播数据传输的中断时间，提高组播数据传输的可靠性。

PIM BFD也适用于共享网段上Assert竞选的过程，可以快速响应Assert Winner接口故障。

### 缺省配置

表4-25列出了PIM BFD检测报文控制参数的缺省配置。

**表 4-25** PIM BFD 检测报文控制参数的缺省配置

| 参数 | 缺省值 |
| --- | --- |
| 最小发送间隔 | 1000ms |
| 最小接收间隔 | 1000ms |
| 本地检测倍数 | 3 |

### 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**interface** *interface-type interface-number*，进入接口视图。

**步骤3** 执行命令**pim bfd enable**，使能PIM BFD功能。

**步骤4** （可选）执行命令**pim bfd** { **min-tx-interval** *tx-value* | **min-rx-interval** *rx-value* | **detect-multiplier** *multiplier-value* } *，调整PIM BFD参数：PIM BFD检测消息的最小发送间隔、最小接收间隔、本地检测倍数。

**----结束**

### 检查配置结果

配置PIM BFD成功后，可以通过以下命令查看PIM BFD session信息。

- **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **bfd session statistics**
- **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **bfd session** [ **interface** *interface-type interface-number* | **neighbor** *neighbor-address* ] *

## 4.8.11 配置 PIM Silent

设备直连用户主机的接口上需要使能PIM协议，当恶意主机模拟PIM Hello报文，大量发送时，有可能导致设备瘫痪。为了避免这样的情况发生，可以将该接口设置为PIM Silent状态。

### 前置任务

在配置PIM Silent之前，需完成以下任务：

- 配置单播路由协议，保证网络内单播路由畅通。
- **使能PIM-SM**。

### 背景信息

在接入层上，设备直连用户主机的接口上如果需要使能PIM协议，在该接口上可以建立PIM邻居，处理各类PIM协议报文。此配置同时存在着安全隐患：当恶意主机模拟发送PIM Hello报文时，有可能导致设备瘫痪。

为了避免这样的情况发生，可以将该接口设置为PIM Silent状态（即PIM消极状态）。当接口进入PIM消极状态后，禁止接收和转发任何PIM协议报文，删除该接口上的所有

PIM邻居以及PIM状态机，该接口作为静态DR立即生效。同时，该接口上的IGMP功能不受影响。

该功能仅适用于与用户主机网段直连的PIM设备接口，且该用户网段只与这一台PIM设备相连。

注意

- 配置了该功能后，接口将不再接收和转发任何PIM协议报文，即该接口配置的其他PIM功能将失效，请谨慎使用。
- 如果用户网段与多台PIM设备相连，在多个PIM设备接口上配置PIM Silent，则这些接口都成为了静态DR，将导致该网段中同时存在多个DR，从而引发组播故障。

### 操作步骤

**步骤1** 执行命令**system-view**，进入系统视图。

**步骤2** 执行命令**interface** *interface-type interface-number*，进入接口视图。

**步骤3** 执行命令**pim silent**，使能PIM Silent功能。

**----结束**

### 检查配置结果

配置PIM Silent成功后，可以通过命令查看PIM接口信息。

- 使用**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]查看接口上的PIM信息。

## 4.9 维护 PIM-DM

PIM-DM的维护包括：清除PIM控制报文统计信息、监控PIM的运行状况。

## 4.9.1 清除 PIM 控制报文统计信息

### 背景信息

如果当前接口使能了PIM协议之后很长时间没有中断组播报文的转发，设备将会存储大量该接口下的控制报文的统计信息。此时可以将已有PIM控制报文统计数清零，重新统计PIM控制报文数量。此操作不影响PIM的正常运行。

注意

清除接口上的PIM控制报文统计信息后，以前的统计信息将无法恢复，务必仔细确认。

### 操作步骤

- 在确认需要清除接口上的PIM控制报文统计信息后，请在用户视图下执行**reset pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **control-message counters** [ **interface** *interface-type interface-number* ]命令。

**----结束**

## 4.9.2 监控 PIM 的运行状况

### 背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解PIM的运行状况。

### 操作步骤

- 执行命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **claimed-route** [ *source-address* ]，查看PIM使用的单播路由信息。
- 执行命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **control-message counters** [ **message-type** { **assert** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** | **bsr** } | **interface** *interface-type interface-number* ] *，查看发送和接收PIM控制报文的数目信息。
- 执行命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]，查看接口上的PIM信息。
- 执行命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **neighbor** [ *neighbor-address* | **interface** *interface-type interface-number* | **verbose** ] *，查看PIM邻居信息。
- 执行以下命令，查看PIM协议组播路由表的内容：
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm** ] * [ **outgoing-interface-number** [ *number* ] ]
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table brief** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } ] *
- 执行命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **invalid-packet** [ **interface** *interface-type interface-number* | **message-type** { **assert** | **hello** | **join-prune** | **graft** | **graft-ack** | **state-refresh** } ] *，查看设备接收到的无效PIM报文的统计信息。

**----结束**

# 4.10 维护 PIM-SM

PIM-SM的维护包括：清除PIM控制报文统计信息、清除PIM路由表项下游接口的状态、监控PIM的运行状况。

## 4.10.1 清除 PIM 控制报文统计信息

### 背景信息

需要重新统计PIM控制报文数量时，可以将已有PIM控制报文统计数清零，注意清除后无法恢复。此操作不影响PIM的正常运行。

注意

清除接口上的PIM控制报文统计信息后，以前的统计信息将无法恢复，务必仔细确认。

### 操作步骤

- 在用户视图下执行命令**reset pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **control-message counters** [ **interface** *interface-type interface-number* ]，清除接口上的PIM控制报文统计信息。

----结束

## 4.10.2 清除 PIM 表项的指定下游接口的 PIM 状态

### 背景信息

可以根据需要清除指定PIM表项的指定下游接口的PIM状态，同时不影响该接口上的IGMP和静态组状态。

注意

清除下游接口的PIM状态后，可能会触发发送相应的Join/Prune报文，影响组播业务。

### 操作步骤

- 在确认需要清除指定PIM表项的指定下游接口的PIM状态后，请在用户视图下执行**reset pim** [ **vpn-instance** *vpn-instance-name* ] **routing-table group** *group-address* **mask** { *group-mask-length* | *group-mask* } **source** *source-address* **interface** *interface-type interface-number*命令。

----结束

## 4.10.3 监控 PIM 的运行状况

### 背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解PIM的运行状况。

## 操作步骤

- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **claimed-route** [ *source-address* ]，查看PIM使用的单播路由信息。
- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **bfd session** [ **interface** *interface-type interface-number* | **neighbor** *neighbor-address* ] *，查看PIM BFD session的信息。
- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **bsr-info**，查看PIM-SM域中BSR的信息。
- 使用以下命令，查看发送和接收PIM控制报文的数目信息。
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **control-message counters message-type** { **probe** | **register** | **register-stop** | **crp** }
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **control-message counters** [ **message-type** { **assert** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** | **bsr** } | **interface** *interface-type interface-number* ] *
- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **interface** [ *interface-type interface-number* | **up** | **down** ] [ **verbose** ]，查看接口上的PIM信息。
- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **neighbor** [ *neighbor-address* | **interface** *interface-type interface-number* | **verbose** ] *，查看PIM邻居信息。
- 使用以下命令查看PIM路由表：
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm** ] * [ **outgoing-interface-number** [ *number* ] ]
  - **display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **routing-table brief** [ *group-address* [ **mask** { *group-mask-length* | *group-mask* } ] | *source-address* [ **mask** { *source-mask-length* | *source-mask* } ] | **incoming-interface** { *interface-type interface-number* | **register** } ] *
- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **rp-info** [ *group-address* ]命令，查看组播组对应的RP信息。
- 使用命令**display pim** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **invalid-packet** [ **interface** *interface-type interface-number* | **message-type** { **assert** | **bsr** | **hello** | **join-prune** | **graft** | **graft-ack** | **state-refresh** } ] *命令，查看设备接收到的无效PIM报文的统计信息。

**----结束**

# 4.11 PIM（IPv4）配置举例

介绍PIM（IPv4）协议常用功能的配置示例。

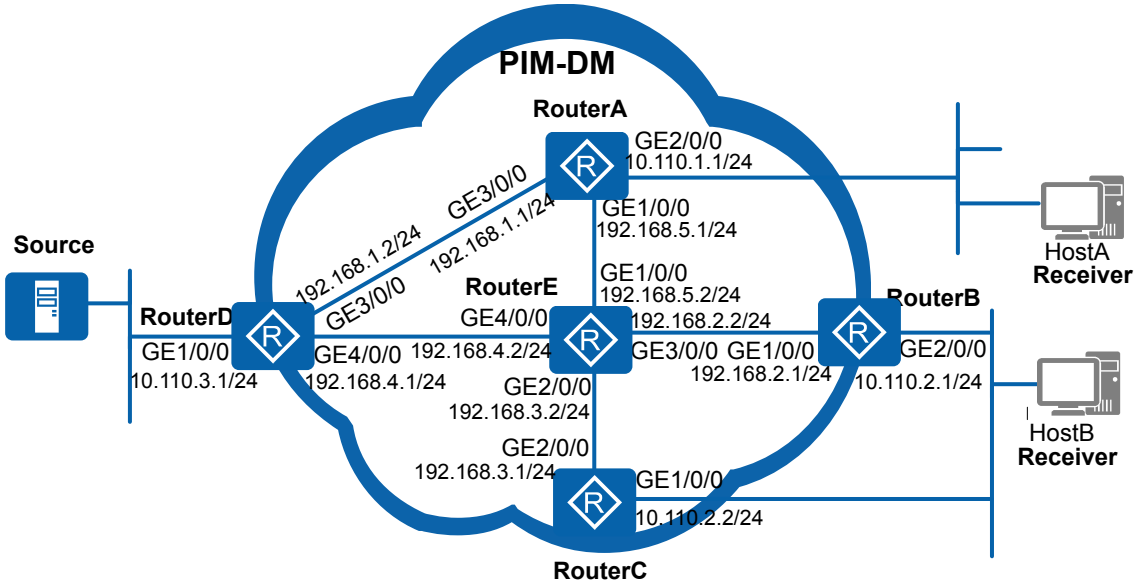
## 4.11.1 配置 PIM-DM 基本网络示例

## 组网需求

如图4-19所示的一个用户比较密集的小型网络，用户主机HostA、HostB希望能够接收到Source发送的组播数据信息。

**图 4-19** 配置 PIM-DM 基本功能的组网图




## 配置思路

由于网络中用户密集，可以使用PIM-DM协议为网络中的用户主机提供组播服务，使得加入同一组播组的所有用户主机能够接收组播源发往该组的视频点播信息。

1. 配置路由器接口IP地址和单播路由协议。组播域内路由协议PIM依赖单播路由协议，单播路由正常是组播协议正常工作的基础。
2. 在所有提供组播服务的路由器上使能组播路由功能。使能组播路由功能是配置PIM-DM的前提。
3. 在路由器所有接口上使能PIM-DM功能。使能PIM-DM功能之后才能配置PIM-DM的其他功能。
4. 在与主机侧相连的路由器接口上使能IGMP。IGMP用于维护组成员关系。叶结点路由器通过IGMP协议来维护组成员关系列表。

   **说明**

   如果用户主机侧需同时配置PIM-DM和IGMP，必须先使能PIM-DM，再使能IGMP。

## 操作步骤

**步骤1** 配置各接口的IP地址和单播路由协议。

# 配置各路由器接口的IP地址和掩码，配置各路由器间采用OSPF进行互连，确保网络中各路由器间能够在网络层互通，并且之间能够借助单播路由协议实现动态路由更新。RouterB、RouterC、RouterD和RouterE上的配置过程与RouterA上的配置相似，配置过程略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.5.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.110.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet3/0/0] quit
[RouterA] ospf 100
[RouterA-ospf-100] area 0
[RouterA-ospf-100-area-0.0.0.0] network 192.168.5.0 0.0.0.255
[RouterA-ospf-100-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-100-area-0.0.0.0] network 10.110.1.0 0.0.0.255
```

**步骤2** 使能组播功能，在各接口上使能PIM-DM功能。

# 在所有路由器使能组播功能，在各接口上使能PIM-DM功能。RouterB、RouterC、RouterD和RouterE上的配置过程与RouterA上的配置相似，配置过程略。

```
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] pim dm
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] pim dm
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] pim dm
[RouterA-GigabitEthernet3/0/0] quit
```

**步骤3** 在连接用户主机的接口上使能IGMP功能。

# 在RouterA连接用户主机的接口上使能IGMP功能。RouterB和RouterC上的配置过程与RouterA上的配置相似，配置过程略。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] igmp enable
```

**步骤4** 验证配置结果。

# 使用命令**display pim interface**命令查看接口上PIM的配置和运行情况。例如RouterC上PIM的显示信息如下，表明接口上的PIM协议已经运行：

```
<RouterC> display pim interface
VPN-Instance: public net
Interface      State   NbrCnt   HelloInt   DR-Pri     DR-Address
GE1/0/0        up      0         30         1         10.110.2.2     (local)
GE2/0/0        up      1         30         1         192.168.3.2
```

# 使用命令**display pim routing-table**查看PIM协议组播路由表。组播源（10.110.3.100/24）向组播组（225.1.1.1/24）发送信息，HostA、HostB都加入了组播组（225.1.1.1/24）。显示信息如下：

```
[RouterA] display pim routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry
 (10.110.3.100, 225.1.1.1)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:00:29
     Upstream interface: GigabitEthernet3/0/0
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
    Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/0
```

```
            Protocol: pim-dm, UpTime: 00:00:29, Expires:-
[RouterB] display pim routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry
 (10.110.3.100, 225.1.1.1)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:00:29
     Upstream interface: GigabitEthernet1/0/0
         Upstream neighbor: 192.168.2.2
         RPF prime neighbor: 192.168.2.2
    Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/0
             Protocol: pim-dm, UpTime: 00:00:30, Expires:-
[RouterD] display pim routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry
 (10.110.3.100, 225.1.1.1)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:00:29
     Upstream interface: GigabitEthernet1/0/0
         Upstream neighbor: 10.110.3.100
         RPF prime neighbor: 10.110.3.100
     Downstream interface(s) information:
     Total number of downstreams: 2
         1: GigabitEthernet3/0/0
         1: GigabitEthernet4/0/0
             Protocol: pim-dm, UpTime: 00:00:29, Expires:-
[RouterE] display pim routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry
 (10.110.3.100, 225.1.1.1)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:01:22
     Upstream interface: GigabitEthernet4/0/0
         Upstream neighbor: 192.168.4.1
         RPF prime neighbor: 192.168.4.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet3/0/0
             Protocol: pim-dm, UpTime: 00:01:22, Expires:-
[RouterC] display pim routing-table
 VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry
 (10.110.3.100, 225.1.1.1)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:01:25
     Upstream interface: GigabitEthernet2/0/0
         Upstream neighbor: 192.168.3.2
         RPF prime neighbor: 192.168.3.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/0
             Protocol: pim-dm, UpTime: 00:01:25, Expires:-
```

**----结束**

# 配置文件

- RouterA的配置文件

```
#
 sysname RouterA
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.5.1 255.255.255.0
 pim dm
```

```
#
interface GigabitEthernet2/0/0
 ip address 10.110.1.1 255.255.255.0
 pim dm
 igmp enable
#
interface GigabitEthernet3/0/0
 ip address 192.168.1.1 255.255.255.0
 pim dm
#
ospf 1
 area 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.5.0 0.0.0.255
#
return
```

- RouterB的配置文件

```
#
 sysname RouterB
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.1 255.255.255.0
 pim dm
#
interface GigabitEthernet2/0/0
 ip address 10.110.2.1 255.255.255.0
 pim dm
 igmp enable
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
return
```

- RouterC的配置文件

```
#
 sysname RouterC
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.110.2.2 255.255.255.0
 pim dm
 igmp enable
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.1 255.255.255.0
 pim dm
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
return
```

- RouterD的配置文件

```
#
 sysname RouterD
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.110.3.1 255.255.255.0
```

```
 pim dm
#
interface GigabitEthernet3/0/0
 ip address 192.168.1.2 255.255.255.0
 pim dm
#
interface GigabitEthernet4/0/0
 ip address 192.168.4.1 255.255.255.0
 pim dm
#
ospf 1
 area 0.0.0.0
  network 10.110.3.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
return
```

- RouterE的配置文件

```
#
 sysname RouterE
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.5.2 255.255.255.0
 pim dm
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.2 255.255.255.0
 pim dm
#
interface GigabitEthernet3/0/0
 ip address 192.168.2.2 255.255.255.0
 pim dm
#
interface GigabitEthernet4/0/0
 ip address 192.168.4.2 255.255.255.0
 pim dm
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
  network 192.168.5.0 0.0.0.255
#
return
```

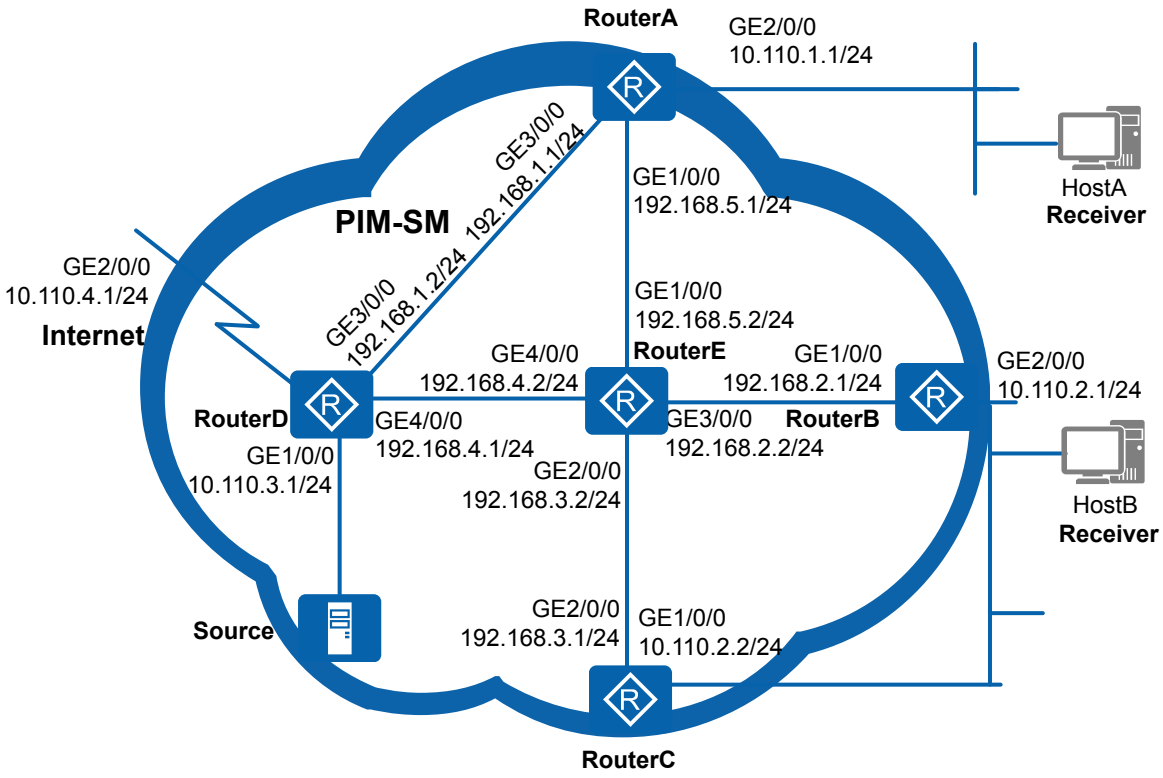
## 4.11.2 配置 ASM 的 PIM-SM 网络示例

### 组网需求

如图4-20所示，该网络接入了Internet。要求通过在路由器配置PIM-SM协议，为网络中的用户主机提供ASM服务，使得加入同一组播组的所有用户主机能够接收任意源发往该组的组播数据信息。

**图 4-20** 配置 ASM 模型的 PIM-SM 域内组播组网图




## 配置思路

1. 配置路由器接口IP地址和单播路由协议。组播域内路由协议PIM依赖单播路由协议，单播路由正常是组播协议正常工作的基础。
2. 在所有提供组播服务的路由器上使能组播功能。使能组播功能是配置PIM-SM的前提。
3. 在路由器所有接口上使能PIM-SM功能。使能PIM-SM功能之后才能配置PIM-SM的其他功能。
4. 在与主机侧相连的路由器接口上使能IGMP。接收者能通过发送IGMP消息自由加入或者离开某个组播组。叶结点路由器通过IGMP协议来维护组成员关系列表。

   **说明**

   如果用户主机侧需同时配置PIM-SM和IGMP，必须先使能PIM-SM，再使能IGMP。
5. 在与主机侧相连的路由器接口上使能PIM Silent，防止恶意主机模拟发送PIM Hello报文，增加PIM-SM域的安全性。

   **说明**

   如果用户主机所在网段相连着多台路由器，那么这些路由器的用户主机侧接口不能使能PIM Silent，如本图中的RouterB、RouterC的位置。
6. 配置RP。在PIM-SM域中，RP是提供ASM服务的核心，是转发组播数据的中转站。建议RP的位置配置在组播流量分支较多的路由器上，如图4-20中的RouterE的位置。
7. 在与Internet相连的接口上配置BSR边界，自举报文不能通过该边界，使BSR只为该PIM-SM域服务，增加组播可控性。

## 操作步骤

**步骤1** 配置各接口的IP地址和单播路由协议。

# 按照图4-20配置各路由器接口的IP地址和掩码，配置各路由器间采用OSPF进行互连，确保网络中各路由器间能够在网络层互通，并且之间能够借助单播路由协议实现动态路由更新。RouterB、RouterC、RouterD和RouterE上的配置过程与RouterA上的配置相似，配置过程略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.5.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.110.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet3/0/0] quit
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.110.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.5.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

**步骤2** 使能组播功能，在各接口上使能PIM-SM功能。

# 在所有路由器使能组播功能，在各接口上使能PIM-SM功能。RouterB、RouterC、RouterD和RouterE上的配置过程与RouterA上的配置相似，配置过程略。

```
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] pim sm
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] pim sm
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] pim sm
[RouterA-GigabitEthernet3/0/0] quit
```

**步骤3** 在连接用户主机的接口上使能IGMP功能。

# 在RouterA连接用户主机的接口上使能IGMP功能。RouterB和RouterC上的配置过程与RouterA上的配置相似，配置过程略。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] igmp enable
```

**步骤4** 在RouterA接口上使能PIM silent。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] pim silent
```

**步骤5** 配置RP。

**说明**

配置RP有两种方式：静态RP和动态RP两种。可以同时配置，也可以只配置其中一种。同时配置两种RP时，可以通过参数调整优先选择哪种RP。

本实例同时配置两种RP，默认优选动态RP，静态RP作为备份。

# 配置动态RP。需要将PIM-SM域的一个或多个路由器上配置为C-RP和C-BSR。本例中指定RouterE同时为C-RP和C-BSR，在RouterE上配置RP服务的组地址范围，及C-BSR和C-RP所在接口位置。

```
[RouterE] acl number 2008
[RouterE-acl-basic-2008] rule permit source 225.1.1.0 0.0.0.255
[RouterE-acl-basic-2008] quit
[RouterE] pim
[RouterE-pim] c-bsr gigabitethernet 4/0/0
[RouterE-pim] c-rp gigabitethernet 4/0/0 group-policy 2008
```

# 配置静态RP。需要在所有路由器上指定静态RP的地址，在RouterA上配置如下。RouterB、RouterC、RouterD和RouterE上的配置过程与RouterA上的配置相似，配置过程略。

**说明**

如果命令**static-rp X.X.X.X**后面选择参数preferred，优先选择静态RP作为本PIM-SM域的RP。

```
[RouterA] pim
[RouterA-pim] static-rp 192.168.2.2
```

**步骤6** 在RouterD与Internet相连的接口上配置BSR边界。

```
[RouterD] interface gigabitethernet 2/0/0
[RouterD-GigabitEthernet2/0/0] pim bsr-boundary
[RouterD-GigabitEthernet2/0/0] quit
```

**步骤7** 验证配置结果。

# 通过使用**display pim interface**命令可以查看接口上PIM的配置和运行情况。例如RouterC上PIM的显示信息如下：

```
<RouterC> display pim interface
VPN-Instance: public net
Interface      State   NbrCnt   HelloInt   DR-Pri     DR-Address
GE1/0/0         up      0          30         1         10.110.2.2     (local)
GE2/0/0         up      1          30         1         192.168.3.2
```

# 通过使用**display pim bsr-info**命令可以查看路由器上BSR选举的信息。例如RouterA和RouterE上BSR信息分别如下（RouterE上还显示C-BSR信息）：

```
<RouterA> display pim bsr-info
VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: 192.168.4.2
     Priority: 0
     Hash mask length: 30
     State: Accept Preferred
     Scope: Not scoped
     Uptime: 01:40:40
     Expires: 00:01:42
     C-RP Count: 1

<RouterE> display pim bsr-info
VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: 192.168.4.2
     Priority: 0
     Mask length: 30
     State: Elected
     Scope: Not scoped
     Uptime: 00:00:18
     Next BSR message scheduled at :00:01:42
     C-RP Count: 1
 Candidate AdminScoped BSR Count: 0
 Candidate BSR Address is: 192.168.4.2
     Priority: 0
     Hash mask length: 30
```

```
    State:Elected
    Scope: Not scoped
    Wait to be BSR: 0
```

# 通过使用**display pim rp-info**命令可以查看Router上获取的RP信息。例如RouterA上RP信息如下：

```
<RouterA> display pim rp-info
VPN-Instance: public net
 PIM-SM BSR RP Number:1
 Group/MaskLen: 225.1.1.0/24
     RP: 192.168.4.2
     Priority: 0
     Uptime: 00:45:13
     Expires: 00:02:17
 PIM SM static RP Number:1
     Static RP: 192.168.2.2
```

# 通过使用**display pim routing-table**命令可以查看PIM协议组播路由表。组播源（10.110.3.100/24）向组播组（225.1.1.1/24）发送信息，HostA、HostB都加入了组播组（225.1.1.1/24）。以RouterA和RouterB为例，显示信息如下：

**说明**

缺省情况下，组成员端DR在收到组播源发来的第一份组播数据后就会触发SPT切换，新建（S，G）路由表项。因此，路由器上显示的（S，G）路由表项一般都是SPT切换后的（S，G）路由表项。

```
[RouterA] display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
     RP: 192.168.4.2
     Protocol: pim-sm, Flag: WC
     UpTime: 00:13:46
     Upstream interface: GigabitEthernet3/0/0
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/0
             Protocol: igmp, UpTime: 00:13:46, Expires:-

(10.110.3.100, 225.1.1.1)
     RP: 192.168.4.2
     Protocol: pim-sm, Flag: SPT ACT
     UpTime: 00:00:42
     Upstream interface: GigabitEthernet1/0/0
         Upstream neighbor: 192.168.5.2
         RPF prime neighbor: 192.168.5.2
    Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/0
             Protocol: pim-sm, UpTime: 00:00:42, Expires:-
[RouterB] display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
     RP: 192.168.4.2
     Protocol: pim-sm, Flag: WC
     UpTime: 00:10:12
     Upstream interface: GigabitEthernet1/0/0
         Upstream neighbor: 192.168.2.2
         RPF prime neighbor: 192.168.2.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/0
```

```
            Protocol: igmp, UpTime: 00:10:12, Expires:-

(10.110.3.100, 225.1.1.1)
     RP: 192.168.4.2
     Protocol: pim-sm, Flag: SPT ACT
     UpTime: 00:00:42
     Upstream interface: GigabitEthernet1/0/0
         Upstream neighbor: 192.168.2.2
         RPF prime neighbor: 192.168.2.2
    Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/0
             Protocol: pim-sm, UpTime: 00:00:30, Expires:-
```

**----结束**

# 配置文件

- RouterA的配置文件

```
#
 sysname RouterA
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.5.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 10.110.1.1 255.255.255.0
 pim silent
 pim sm
 igmp enable
#
interface GigabitEthernet3/0/0
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.5.0 0.0.0.255
#
pim
 static-rp 192.168.2.2
#
return
```

- RouterB的配置文件

```
#
 sysname RouterB
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 10.110.2.1 255.255.255.0
 pim sm
 igmp enable
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
```

```
  network 192.168.2.0 0.0.0.255
#
pim
 static-rp 192.168.2.2
#
return
```

- RouterC的配置文件

```
#
 sysname RouterC
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.110.2.2 255.255.255.0
 pim sm
 igmp enable
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
pim
 static-rp 192.168.2.2
#
return
```

- RouterD的配置文件

```
#
 sysname RouterD
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.110.3.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 10.110.4.1 255.255.255.0
 pim bsr-boundary
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface GigabitEthernet4/0/0
 ip address 192.168.4.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.3.0 0.0.0.255
  network 10.110.4.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
 static-rp 192.168.2.2
#
return
```

- RouterE的配置文件

```
#
 sysname RouterE
```

```
#
multicast routing-enable
#
acl number 2008
 rule 5 permit source 225.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 192.168.5.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface GigabitEthernet4/0/0
 ip address 192.168.4.2 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
  network 192.168.5.0 0.0.0.255
#
pim
 c-bsr GigabitEthernet4/0/0
 c-rp GigabitEthernet4/0/0 group-policy 2008
 static-rp 192.168.2.2
#
return
```

## 4.11.3 配置 PIM-SM 域组播 SPT 切换示例

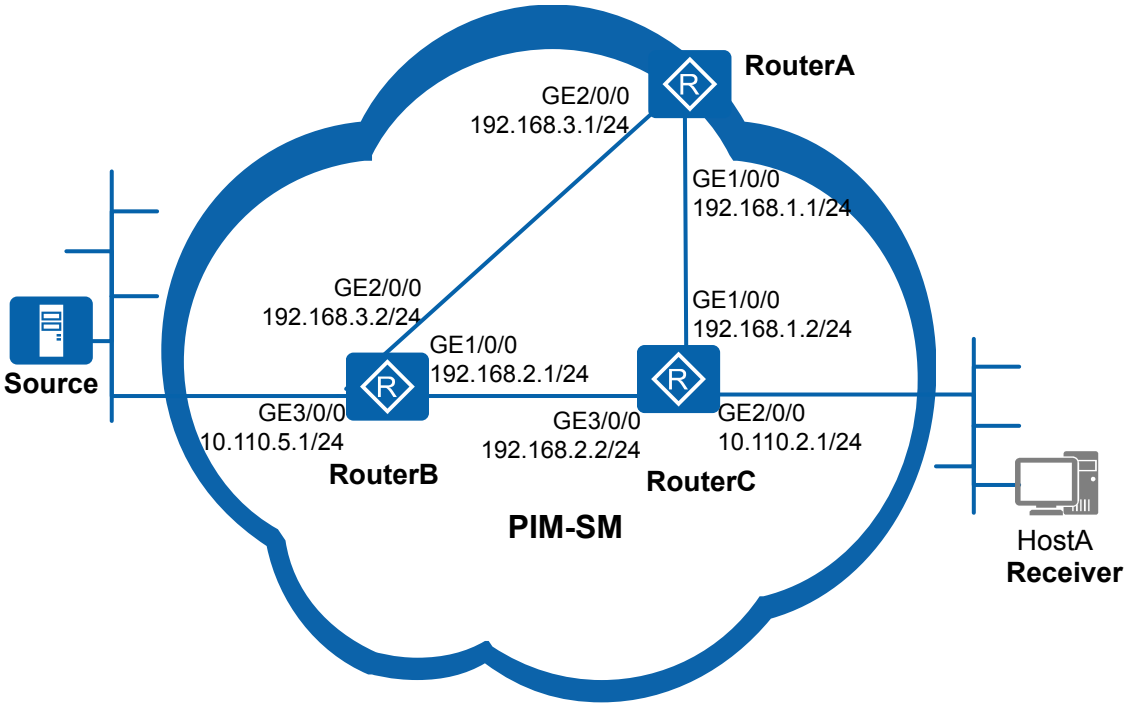
### 组网需求

接收者通过组播方式接收组播数据信息，整个PIM网络采用SM单BSR管理域方式。在缺省情况下，RP和接收者侧DR在收到第一个组播数据包后立即进行SPT切换，寻找最佳路径接收组播源的组播信息。如果接收者希望流量达到阈值以后再进行SPT切换，就需要进行SPT切换的配置。

如图4-21所示，要求通过在路由器进行适当配置，实现末梢网络中的HostA从RP（RouterA的GE1/0/0）上接收组播数据，当组播数据报文速率达到1024kbit/s以后再进行SPT切换（SPT切换后HostA的接收路径是Source-RouterB-RouterC--HostA）。

**图 4-21** 配置 PIM-SM 域组播进行 SPT 切换组网图




## 配置思路

采用如下的思路配置PIM-SM的基本功能：

1. 配置各路由器接口IP地址和单播路由协议。
2. 使能组播功能，在各接口上使能PIM-SM功能，主机侧接口上使能IGMP功能。
3. 在各路由器上配置相同的静态RP。
4. 在RouterC上进行SPT切换相关配置。

## 操作步骤

**步骤1** 配置各路由器接口IP地址和单播路由协议。

# 按照图4-21配置各路由器接口的IP地址和掩码，配置各路由器间采用OSPF进行互连，确保网络中RouterA、RouterB、RouterC之间能够在网络层互通，并且之间能够借助单播路由协议实现动态路由更新。RouterA、RouterB上的配置过程与RouterC上的配置相似，配置过程略。

```
<Huawei> system-view
[Huawei] sysname RouterC
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ip address 192.168.1.2 24
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] ip address 10.110.2.1 24
[RouterC-GigabitEthernet2/0/0] quit
[RouterC] interface gigabitethernet 3/0/0
[RouterC-GigabitEthernet3/0/0] ip address 192.168.2.2 24
[RouterC-GigabitEthernet3/0/0] quit
[RouterCA] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 10.110.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
```

```
[RouterC-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

**步骤2** 使能组播功能，在各接口上使能PIM-SM功能，主机侧接口上使能IGMP功能。

# 在所有路由器使能组播功能，在各接口上使能PIM-SM功能，并在RouterC连接末梢网络的接口上使能IGMP功能。RouterA、RouterB上的配置过程与RouterC上的配置相似，配置过程略。

```
[RouterC] multicast routing-enable
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] pim sm
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] pim sm
[RouterC-GigabitEthernet2/0/0] igmp enable
[RouterC-GigabitEthernet2/0/0] quit
[RouterC] interface gigabitethernet 3/0/0
[RouterC-GigabitEthernet3/0/0] pim sm
[RouterC-GigabitEthernet3/0/0] quit
```

**步骤3** 配置静态RP。

#在RouterA、RouterB和RouterC上配置静态RP。RouterB、RouterC上的配置过程与RouterA上的配置相似，配置过程略。

```
[RouterA] pim
[RouterA-pim] static-rp 192.168.1.1
```

**步骤4** 配置SPT切换阈值。

# 在RouterC上配置组播数据报文速率达到1024kbit/s以后进行SPT切换。

```
[RouterC] pim
[RouterC-pim] spt-switch-threshold 1024
[RouterC-pim] quit
```

**步骤5** 验证配置结果。

# 组播源开始向组播组发送数据，HostA能接收到组播源的数据。当速率小于1024kbit/s的时候，在RouterC上使用**display pim routing-table**命令可以查看PIM协议组播路由表，看到上游邻居是RouterA，显示信息如下：

```
<RouterC> display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
     RP: 192.168.1.1
     Protocol: pim-sm, Flag: WC
     UpTime: 00:13:46
     Upstream interface: GigabitEthernet1/0/0
         Upstream neighbor: 192.168.1.1
         RPF prime neighbor: 192.168.1.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/0
             Protocol: igmp, UpTime: 00:13:46, Expires:-
(10.110.5.100, 225.1.1.1)
     RP: 192.168.1.1
     Protocol: pim-sm, Flag: ACT
     UpTime: 00:00:42
     Upstream interface: GigabitEthernet1/0/0
         Upstream neighbor: 192.168.1.1
         RPF prime neighbor: 192.168.1.1
     Downstream interface(s) information:
     Total number of downstreams: 1
```

```
        1: GigabitEthernet2/0/0
            Protocol: pim-sm, UpTime: 00:00:42, Expires:-
```

# 当速率大于1024kbit/s以后，在RouterC上使用**display pim routing-table**命令可以查看PIM协议组播路由表，看到上游邻居变成了RouterB。显示信息如下：

```
<RouterC> display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
     RP: 192.168.1.1
     Protocol: pim-sm, Flag: WC
     UpTime: 00:13:46
     Upstream interface: GigabitEthernet3/0/0
         Upstream neighbor: 192.168.2.1
         RPF prime neighbor: 192.168.2.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/0,
             Protocol: igmp, UpTime: 00:13:46, Expires:-
(10.110.5.100, 225.1.1.1)
     RP: 192.168.1.1
     Protocol: pim-sm, Flag:RPT SPT ACT
     UpTime: 00:00:42
     Upstream interface: GigabitEthernet3/0/0
         Upstream neighbor: 192.168.2.1
         RPF prime neighbor: 192.168.2.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/0
             Protocol: pim-sm, UpTime: 00:00:42, Expires:-
```

**----结束**

## 配置文件

- RouterA的配置文件

```
#
 sysname RouterA
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
pim
 static-rp 192.168.1.1
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
return
```

- RouterB的配置文件

```
#
 sysname RouterB
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
```

```
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 10.110.5.1 255.255.255.0
 pim sm
#
pim
 static-rp 192.168.1.1
#
ospf 1
 area 0.0.0.0
  network 10.110.5.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
return
```

- RouterC的配置文件

```
#
 sysname RouterC
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 10.110.2.1 255.255.255.0
 pim sm
 igmp enable
#
interface GigabitEthernet3/0/0
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
pim
 spt-switch-threshold 1024
 static-rp 192.168.1.1
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
return
```

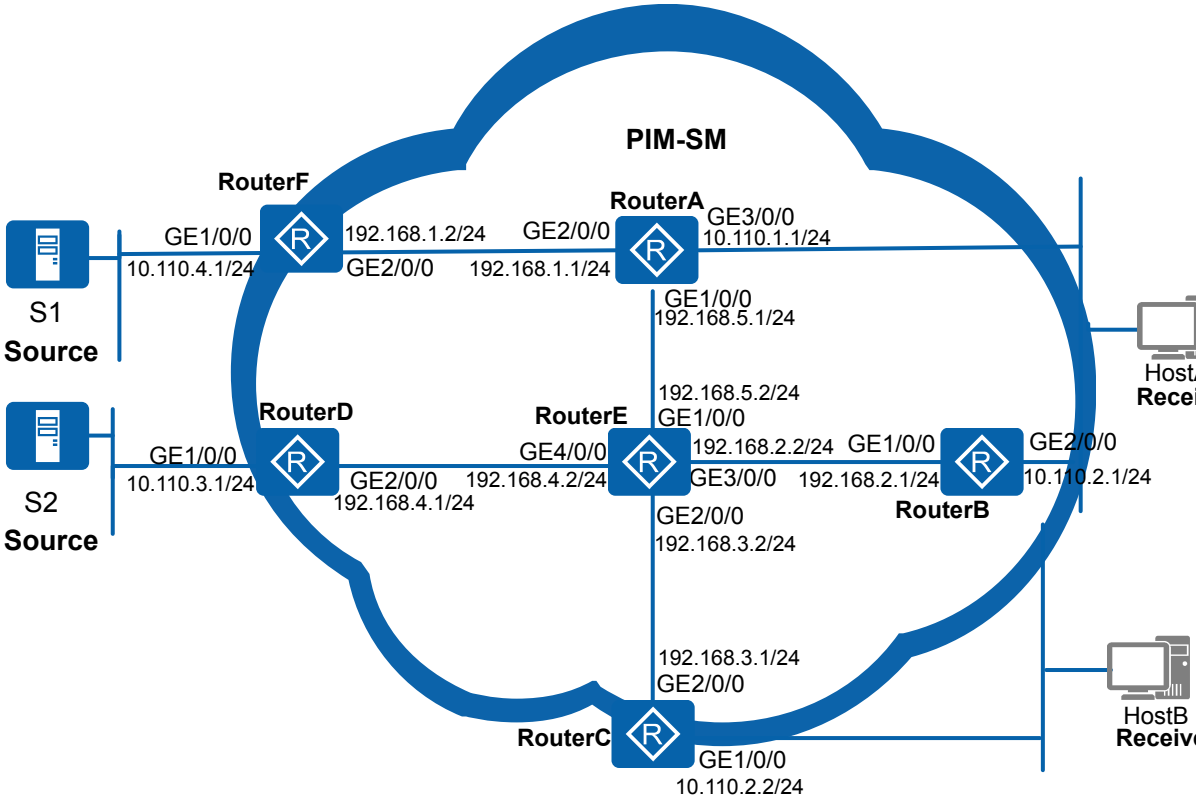
# 4.11.4 配置 SSM 的 PIM-SM 网络示例

## 组网需求

如图4-22所示，要求通过在路由器配置PIM-SM协议，为网络中的用户主机提供SSM服务，使得用户主机在加入组播组的同时，能够接收到自己所指定的组播源的视频点播信息。

**图 4-22** 配置 SSM 模型的 PIM-SM 域内组播组网图




## 配置思路

1. 配置路由器接口IP地址和单播路由协议。组播域内路由协议PIM依赖单播路由协议，单播路由正常是组播协议正常工作的基础。
2. 在所有提供组播服务的路由器上使能组播功能。使能组播功能是配置PIM-SM的前提。
3. 在路由器所有接口上使能PIM-SM功能。使能PIM-SM功能之后才能配置PIM-SM的其他功能。
4. 在与主机侧相连的路由器接口上使能IGMP，并配置IGMP协议的版本号为v3。接收者能通过发送IGMP消息自由加入或者离开指定源的组播组。叶结点路由器通过IGMP协议来维护组成员关系列表。

   **说明**

   如果用户主机侧需同时配置PIM-SM和IGMP，必须先使能PIM-SM，再使能IGMP。

5. 在与主机侧相连的路由器接口上使能PIM Silent，防止恶意主机模拟发送PIM Hello报文，增加PIM-SM域的安全性。

   **说明**

   如果用户主机所在网段相连着多台路由器，那么这些路由器的用户主机侧接口不能使能PIM Silent，如本图中RouterB、RouterC。

6. 在各路由器上设置SSM组地址范围。使PIM-SM域内的路由器为特定组地址范围内的SSM服务，实现可控组播。

**说明**

各路由器上设置SSM组地址范围必须相同。

## 操作步骤

**步骤1** 配置各接口的IP地址和单播路由协议。

# 按照图4-22配置各路由器接口的IP地址和掩码，配置各路由器间采用OSPF进行互连，确保网络中各路由器间能够在网络层互通，并且之间能够借助单播路由协议实现动态路由更新。RouterB、RouterC、RouterD、RouterE和RouterF上的配置过程与RouterA上的配置相似，配置过程略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.5.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.110.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet3/0/0] quit
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.110.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.5.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

**步骤2** 使能组播功能，在各接口上使能PIM-SM功能。

# 在所有路由器使能组播功能，在各接口上使能PIM-SM功能。RouterB、RouterC、RouterD、RouterE和RouterF上的配置过程与RouterA上的配置相似，配置过程略。

```
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] pim sm
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] pim sm
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] pim sm
[RouterA-GigabitEthernet3/0/0] quit
```

**步骤3** 在连接用户主机的接口上使能IGMP功能，并配置IGMP版本号为v3。

# 在RouterA连接用户主机的接口上使能IGMP功能。RouterB和RouterC上的配置过程与RouterA上的配置相似，配置过程略。

```
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] igmp enable
[RouterA-GigabitEthernet3/0/0] igmp version 3
```

**步骤4** 在RouterA接口上使能PIM silent。

```
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] pim silent
```

**步骤5** 配置SSM组播组地址范围。

# 在所有路由器配置SSM组播组地址范围为232.1.1.0/24。RouterB、RouterC、RouterD、RouterE和RouterF上的配置过程与RouterA上的配置完全相同，配置过程略。

```
[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
```

**步骤6** 验证配置结果。

# 通过使用**display pim interface**命令可以查看接口上PIM的配置和运行情况。例如RouterC上PIM的显示信息如下：

```
<RouterC> display pim interface
VPN-Instance: public net
Interface      State   NbrCnt   HelloInt   DR-Pri     DR-Address
GE1/0/0         up      0         30         1         10.110.2.2    (local)
GE2/0/0         up      1         30         1         192.168.3.2
```

# 通过使用**display pim routing-table**命令可以查看PIM协议组播路由表。HostA需要接收组播源（10.110.3.100/24）和组播源（10.110.4.100/24）发往组播组（232.1.1.1/24）的信息，HostB只需要接收组播源（10.110.3.100/24）发往组播组（232.1.1.1/24）的信息，。显示信息如下：

```
[RouterA] display pim routing-table
VPN-Instance: public net
 Total 2 (S, G) entries

(10.110.3.100, 232.1.1.1)
     Protocol: pim-ssm, Flag: SPT ACT
     UpTime: 00:13:46
     Upstream interface: GigabitEthernet2/0/0
         Upstream neighbor: 192.168.5.2
         RPF prime neighbor: 192.168.5.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet3/0/0
             Protocol: igmp, UpTime: 00:13:46, Expires:-

(10.110.4.100, 232.1.1.1)
     Protocol: pim-ssm, Flag: SPT ACT
     UpTime: 00:00:42
     Upstream interface: GigabitEthernet1/0/0
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
    Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet3/0/0
             Protocol: igmp, UpTime: 00:00:42, Expires:-
[RouterB] display pim routing-table
VPN-Instance: public net
 Total 1 (S, G) entry

(10.110.3.100, 232.1.1.1)
     Protocol: pim-ssm, Flag: SPT ACT
     UpTime: 00:10:12
     Upstream interface: GigabitEthernet1/0/0
         Upstream neighbor: 192.168.2.2
         RPF prime neighbor: 192.168.2.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/0
             Protocol: igmp, UpTime: 00:10:12, Expires:-

[RouterC] display pim routing-table
 VPN-Instance: public net
 Total 1 (S, G) entry

 (10.110.3.100, 232.1.1.1)
     Protocol: pim-ssm, Flag:
     UpTime: 00:01:25
```

```
    Upstream interface: GigabitEthernet2/0/0
        Upstream neighbor: 192.168.3.2
        RPF prime neighbor: 192.168.3.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet1/0/0
            Protocol: igmp, UpTime: 00:01:25, Expires:-

[RouterD] display pim routing-table
VPN-Instance: public net
 Total 1 (S, G) entry

 (10.110.3.100, 232.1.1.1)
    Protocol: pim-ssm, Flag: SPT ACT
    UpTime: 00:00:42
    Upstream interface: GigabitEthernet1/0/0
        Upstream neighbor: 10.110.3.100
        RPF prime neighbor: 10.110.3.100
    Downstream interface(s) information:
    Total number of downstreams: 2
        1: GigabitEthernet2/0/0
            Protocol: pim-ssm, UpTime: 00:00:42, Expires:-

[RouterE] display pim routing-table
VPN-Instance: public net
 Total 1 (S, G) entry

 (10.110.3.100, 232.1.1.1)
    Protocol: pim-ssm, Flag: SPT ACT
    UpTime: 00:13:16
    Upstream interface: GigabitEthernet4/0/0
        Upstream neighbor: 192.168.4.1
        RPF prime neighbor: 192.168.4.1
    Downstream interface(s) information:
    Total number of downstreams: 3
        1: GigabitEthernet1/0/0
            Protocol: pim-ssm, UpTime: 00:13:16, Expires: 00:03:20
        2: GigabitEthernet2/0/0
            Protocol: pim-ssm, UpTime: 00:13:16, Expires: 00:03:21
        3: GigabitEthernet3/0/0
            Protocol: pim-ssm, UpTime: 00:13:16, Expires: 00:03:22

[RouterF] display pim routing-table
VPN-Instance: public net
 Total 1 (S, G) entry

 (10.110.4.100, 232.1.1.1)
    Protocol: pim-ssm, Flag: SPT ACT
    UpTime: 00:13:16
    Upstream interface: GigabitEthernet1/0/0
        Upstream neighbor: 10.110.4.100
        RPF prime neighbor: 10.110.4.100
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/0/0
            Protocol: pim-ssm, UpTime: 00:15:28, Expires: 00:05:21
```

**----结束**

# 配置文件

- RouterA的配置文件

```
#
 sysname RouterA
#
multicast routing-enable
#
acl number 2000
```

```
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 192.168.5.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 10.110.1.1 255.255.255.0
 pim silent
 pim sm
 igmp enable
 igmp version 3
#
ospf 1
 area 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.5.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- RouterB的配置文件

```
#
 sysname RouterB
#
multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 10.110.2.1 255.255.255.0
 pim sm
 igmp enable
 igmp version 3
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- RouterC的配置文件

```
#
 sysname RouterC
#
multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 10.110.2.2 255.255.255.0
 pim sm
 igmp enable
```

```
 igmp version 3
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- RouterD的配置文件

```
#
 sysname RouterD
#
multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 10.110.3.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.4.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.3.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- RouterE的配置文件

```
#
 sysname RouterE
#
multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 192.168.5.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface GigabitEthernet4/0/0
 ip address 192.168.4.2 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
```

```
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
  network 192.168.5.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- RouterF的配置文件

```
#
 sysname RouterF
#
multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 10.110.4.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.4.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

## 4.11.5 配置基于 PIM 协议的 Anycast RP 示例

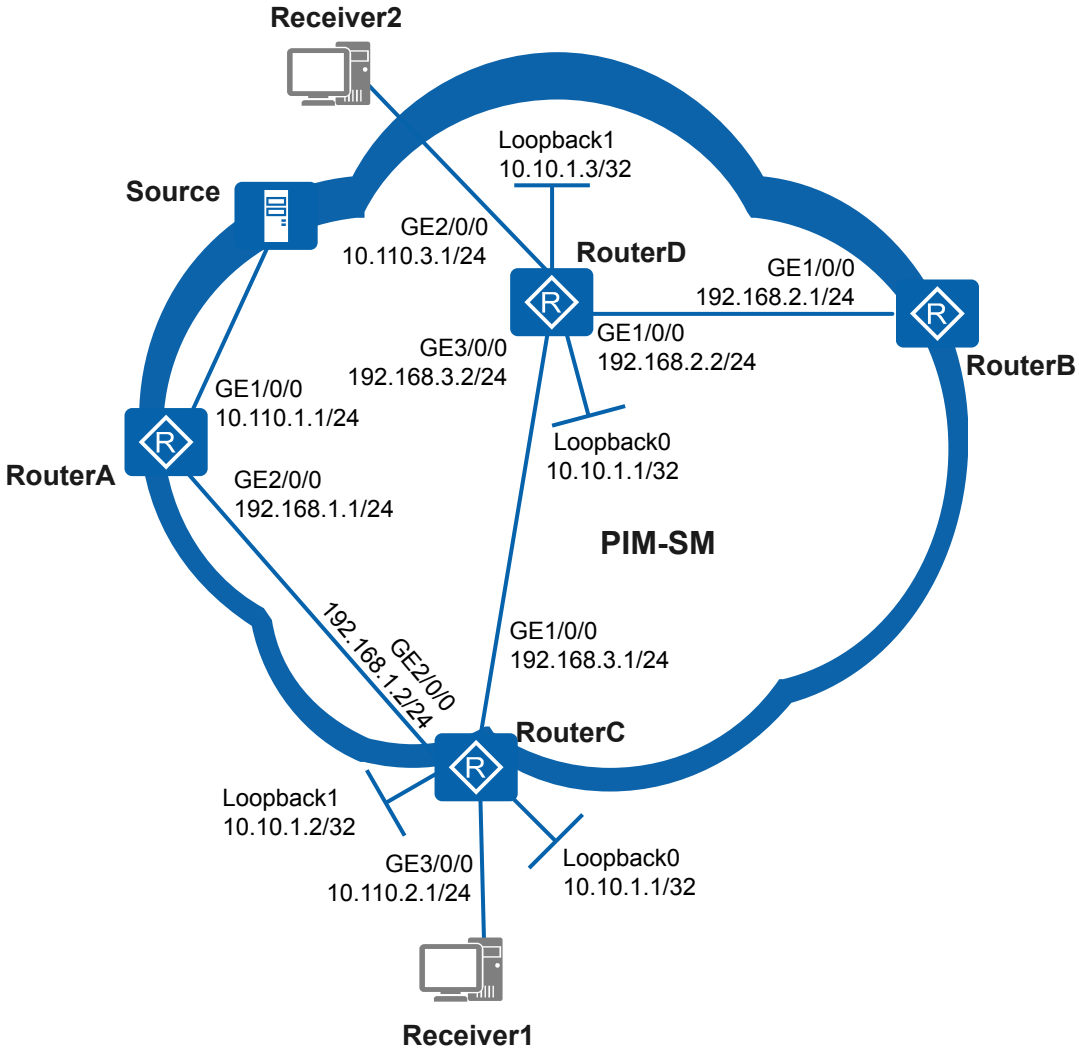
### 组网需求

在传统的PIM-SM域中，每个组播组都只能映射到一个RP。当网络负载较大或流量过于集中时，可能导致RP压力过大、RP失效后路由收敛较慢、组播转发路径非最优等问题。在单自治域中应用基于PIM协议的Anycast RP，可实现组播源就近注册和接收者就近加入。既可以缓解单个RP的负担，也实现了RP备份、优化组播数据的转发路径。

如图4-23所示，Receiver2需要接收Source的组播数据，配置RouterC和RouterD为Anycast RP对等体，Receiver2就近加入RouterD，RouterA收到Source的组播数据后，封装成注册消息向RouterC注册，RouterC收到注册报文后，将注册报文转发给RouterD，Receiver2可以收到组播源的数据。

**图 4-23** 配置基于 PIM 协议的 Anycast RP 组网图




## 配置思路

采用如下的思路配置基于PIM协议的Anycast RP功能：

1. 配置各路由器的接口IP地址，采用OSPF协议实现网络层互通。
2. 使能组播功能，在各接口启动PIM-SM功能。
3. 在路由器与主机侧相连的接口使能IGMP功能。
4. 配置RouterC和RouterD的Loopback0接口为C-RP和C-BSR。
5. 配置RouterC和RouterD的Loopback0接口为Anycast RP。
6. 配置RouterC和RouterD的Loopback1接口为各自的Anycast RP本地地址。
7. 配置RouterC和RouterD互为Anycast RP对等体。

## 操作步骤

**步骤1** 配置各接口的IP地址和单播路由协议

# 按照图4-23配置各路由器接口的IP地址和掩码，配置各路由器间采用OSPF进行互连，确保网络中各路由器间能够在网络层互通，并且之间能够借助单播路由协议实现动态路由更新。RouterB、RouterC和RouterD上的配置过程与RouterA上的配置相似，配置过程略。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 10.110.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.110.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

**步骤2** 使能组播功能，在各接口上使能PIM-SM功能

# 在所有路由器使能组播功能，在各接口上使能PIM-SM功能。RouterB、RouterC和RouterD的配置过程与RouterA上的配置相似，配置过程略。

# 配置RouterA。

```
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] pim sm
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] pim sm
[RouterA-GigabitEthernet2/0/0] quit
```

**步骤3** 在路由器与主机侧相连的接口使能IGMP功能

# 在RouterC和RouterD与主机侧相连的接口使能IGMP功能。

# 配置RouterC。

```
[RouterC] interface gigabitethernet 3/0/0
[RouterC-GigabitEthernet3/0/0] igmp enable
[RouterC-GigabitEthernet3/0/0] quit
```

# 配置RouterD。

```
[RouterD] interface gigabitethernet 2/0/0
[RouterD-GigabitEthernet2/0/0] igmp enable
[RouterD-GigabitEthernet2/0/0] quit
```

**步骤4** 配置RouterC和RouterD的Loopback0接口为C-RP和C-BSR

# 配置RouterC。

```
[RouterC] pim
[RouterC-pim] c-bsr loopback 0
[RouterC-pim] c-rp loopback 0
[RouterC-pim] quit
```

# 配置RouterD。

```
[RouterD] pim
[RouterD-pim] c-bsr loopback 0
```

```
[RouterD-pim] c-rp loopback 0
[RouterD-pim] quit
```

**步骤5** 配置RouterC和RouterD的Loopback0接口为Anycast RP

# 配置RouterC。

```
[RouterC] pim
[RouterC-pim] anycast-rp 10.10.1.1
[RouterC-pim-anycast-rp-10.10.1.1] quit
[RouterC-pim] quit
```

# 配置RouterD。

```
[RouterD] pim
[RouterD-pim] anycast-rp 10.10.1.1
[RouterD-pim-anycast-rp-10.10.1.1] quit
[RouterD-pim] quit
```

**步骤6** 配置RouterC和RouterD的Loopback1接口为各自的Anycast RP本地地址

# 配置RouterC。

```
[RouterC] pim
[RouterC-pim] anycast-rp 10.10.1.1
[RouterC-pim-anycast-rp-10.10.1.1] local-address 10.10.1.2
[RouterC-pim-anycast-rp-10.10.1.1] quit
[RouterC-pim] quit
```

# 配置RouterD。

```
[RouterD] pim
[RouterC-pim] anycast-rp 10.10.1.1
[RouterC-pim-anycast-rp-10.10.1.1] local-address 10.10.1.3
[RouterC-pim-anycast-rp-10.10.1.1] quit
[RouterD-pim] quit
```

**步骤7** 配置RouterC和RouterD互为Anycast RP对等体

# 配置RouterC。

```
[RouterC] pim
[RouterC-pim] anycast-rp 10.10.1.1
[RouterC-pim-anycast-rp-10.10.1.1] peer 10.10.1.3
[RouterC-pim-anycast-rp-10.10.1.1] quit
[RouterC-pim] quit
```

# 配置RouterD。

```
[RouterD] pim
[RouterD-pim] anycast-rp 10.10.1.1
[RouterD-pim-anycast-rp-10.10.1.1] peer 10.10.1.2
[RouterD-pim-anycast-rp-10.10.1.1] quit
[RouterD-pim] quit
```

**步骤8** 验证配置结果

# 通过使用**display pim rp-info**命令可以查看RouterC和RouterD上的RP信息。

```
<RouterC> display pim rp-info
 VPN-Instance: public net
 PIM-SM BSR RP Number:1
 Group/MaskLen: 224.0.0.0/4
     RP: 10.10.1.1 (local)
     Priority: 0
     Uptime: 00:45:19
     Expires: 00:02:11
<RouterD> display pim rp-info
 VPN-Instance: public net
```

```
PIM-SM BSR RP Number:1
Group/MaskLen: 224.0.0.0/4
    RP: 10.10.1.1 (local)
    Priority: 0
    Uptime: 02:27:56
    Expires: 00:01:39
```

由以上显示信息可知，RouterC和RouterD都作为网络中的RP，可以相互转发组播源注册信息。

# 通过使用**display pim routing-table**命令可以查看路由器上的PIM表项。PIM-SM域内组播源Source（10.110.1.2/24）向组播组G（226.1.1.1）发送组播信息，用户Receiver2加入组播组G，接收发往组G的组播数据。Source向RouterC注册，Receiver2向RouterD发起加入。

```
<RouterC> display pim routing-table
 VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry

 (10.110.1.2, 226.1.1.1)
    RP: 10.10.1.1 (local)
    Protocol: pim-sm, Flag: 2MSDP ACT
    UpTime: 00:00:38
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information: None
<RouterD> display pim routing-table
 VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 226.1.1.1)
    RP: 10.10.1.1 (local)
    Protocol: pim-sm, Flag: WC
    UpTime: 00:01:25
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/0/0
            Protocol: igmp, UpTime: 00:01:25, Expires: -

 (10.110.1.2, 226.1.1.1)
    RP: 10.10.1.1 (local)
    Protocol: pim-sm, Flag: 2MSDP SWT ACT
    UpTime: 00:00:02
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/0/0
            Protocol: pim-sm, UpTime: 00:00:02, Expires: -
```

**----结束**

## 配置文件

- RouterA的配置文件

```
#
 sysname RouterA
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.110.1.1 255.255.255.0
```

```
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
#
return
```

- RouterB的配置文件

```
#
 sysname RouterB
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
   network 192.168.2.0 0.0.0.255
#
return
```

- RouterC的配置文件

```
#
 sysname RouterC
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 10.110.2.1 255.255.255.0
 pim sm
 igmp enable
#
interface LoopBack0
 ip address 10.10.1.1 255.255.255.255
 pim sm
#
interface LoopBack1
 ip address 10.10.1.2 255.255.255.255
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 10.110.2.0 0.0.0.255
  network 10.10.1.1 0.0.0.0
  network 10.10.1.2 0.0.0.0
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
 anycast-rp 10.10.1.1
  local-address 10.10.1.2
  peer 10.10.1.3
```

```
#
return
```

- RouterD的配置文件

```
#
 sysname RouterD
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 10.110.3.1 255.255.255.0
 pim sm
 igmp enable
#
interface GigabitEthernet3/0/0
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface LoopBack0
 ip address 10.10.1.1 255.255.255.255
 pim sm
#
interface LoopBack1
 ip address 10.10.1.3 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 10.110.3.0 0.0.0.255
  network 10.10.1.3 0.0.0.0
  network 10.10.1.1 0.0.0.0
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
 anycast-rp 10.10.1.1
  local-address 10.10.1.3
  peer 10.10.1.2
#
return
```

# 4.11.6 配置 PIM GR 示例

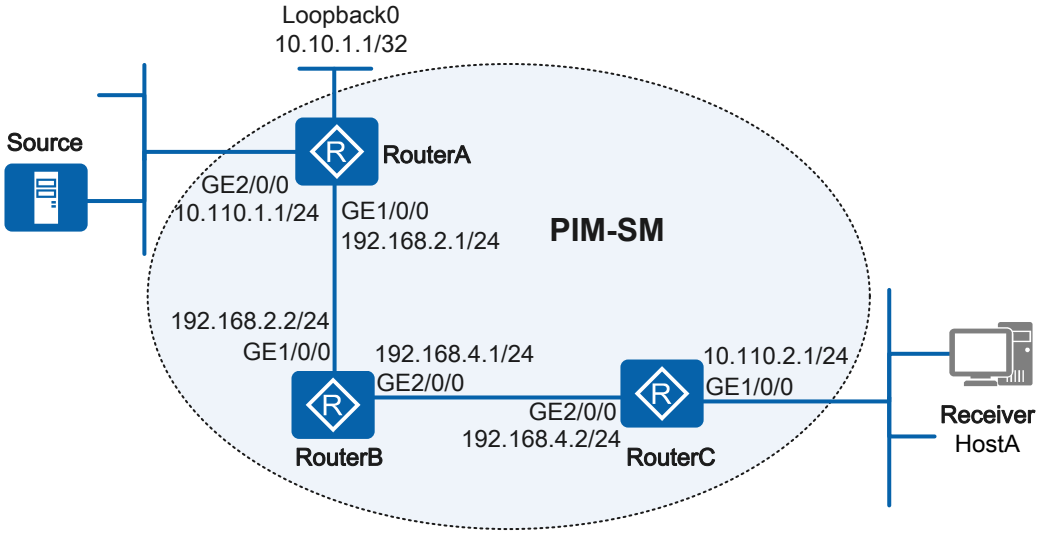
## 组网需求

如图4-24所示的网络中部署了组播业务，PIM-SM网络中的RouterC是具有双主控板的设备，RouterA、RouterB均支持单播GR。

RouterC因为某些原因需要进行主备倒换。要求RouterC在主备倒换期间，接口板能够正常转发组播数据，不会导致下游用户的组播业务中断。

**图 4-24** 配置 PIM GR 组网图




## 配置思路

可以通过配置PIM GR功能实现以上需求。采用如下的思路配置PIM GR的基本功能：

1. 配置路由器各接口的IP地址和单播路由协议。
2. 使能各路由器的单播GR功能，配置单播GR周期。
3. 使能组播功能，在各路由器的接口上使能PIM-SM功能，并在RouterC与主机侧相连的接口使能IGMP。
4. 配置RP。在各路由器上配置相同的静态RP。
5. 在RouterC上使能PIM GR功能，配置GR周期。

## 操作步骤

**步骤1** 配置路由器各接口的IP地址和单播路由协议。

# 按照图4-24配置各路由器接口的IP地址和掩码，各路由器之间采用OSPF进行互连，确保网络中RouterA、RouterB和RouterC之间能够在网络层互通。RouterA和RouterB上的配置过程与RouterC上的配置相似，配置过程略。

```
<Huawei> system-view
[Huawei] sysname RouterC
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ip address 10.110.2.1 24
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] ip address 192.168.4.2 24
[RouterC-GigabitEthernet2/0/0] quit
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 10.110.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 192.168.4.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

**步骤2** 使能各路由器的单播GR功能，配置单播GR周期。

# 在所有路由器上使能单播GR功能，配置单播GR周期为200秒。RouterA、RouterB上的配置过程与RouterC上的配置相似，配置过程略。

```
[RouterC] ospf
[RouterC-ospf-1] opaque-capability enable
[RouterC-ospf-1] graceful-restart
[RouterC-ospf-1] graceful-restart period 200
[RouterC-ospf-1] quit
```

**步骤3** 使能组播功能，在各路由器的接口上使能PIM-SM，并在RouterC与主机侧相连的接口上使能IGMP。

# 在所有路由器上使能组播功能，在各路由器的接口上使能PIM-SM功能。RouterA、RouterB上的配置过程与RouterC上的配置相似，配置过程略。

```
[RouterC] multicast routing-enable
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] pim sm
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] pim sm
[RouterC-GigabitEthernet2/0/0] quit
```

# 在RouterC与主机侧相连的接口上使能IGMP。

```
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] igmp enable
[RouterC-GigabitEthernet1/0/0] quit
```

**步骤4** 配置静态RP。

**说明**

由于本地Loopback接口永远处于up状态，稳定性高，推荐配置静态RP的地址为Loopback接口的地址。

# 在所有路由器上配置静态RP。RouterA、RouterB上的配置过程与RouterC上的配置相似，配置过程略。

```
[RouterC] pim
[RouterC-pim] static-rp 10.10.1.1
[RouterC-pim] quit
```

**步骤5** 使能PIM GR功能，配置PIM GR周期。

# 在RouterC上使能PIM GR功能，配置PIM GR周期为300秒。

```
[RouterC] pim
[RouterC-pim] graceful-restart
[RouterC-pim] graceful-restart period 300
[RouterC-pim] quit
```

**步骤6** 验证配置结果。

# 组播源（10.110.1.100）向组播组（225.1.1.1）发送数据，HostA发送IGMP报告报文加入组播组，并能接收到组播源的数据。RouterC主备倒换前，在RouterB和RouterC上分别使用**display pim routing-table**命令查看路由表，显示信息如下：

```
<RouterB> display pim routing-table
 VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 225.1.1.1)
     RP: 10.10.1.1
     Protocol: pim-sm, Flag: WC
     UpTime: 01:52:38
     Upstream interface: GigabitEthernet1/0/0
         Upstream neighbor: 192.168.2.1
```

```
        RPF prime neighbor: 192.168.2.1
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/0/0
            Protocol: pim-sm, UpTime: 01:52:38, Expires: 00:02:53

 (10.110.1.100, 225.1.1.1)
    RP: 10.10.1.1
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 01:52:38
    Upstream interface: GigabitEthernet1/0/0
        Upstream neighbor: 192.168.2.1
        RPF prime neighbor: 192.168.2.1
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/0/0
            Protocol: pim-sm, UpTime: 01:52:38, Expires: 00:03:03
<RouterC> display pim routing-table
 VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 225.1.1.1)
    RP: 10.10.1.1
    Protocol: pim-sm, Flag: WC
    UpTime: 01:51:24
    Upstream interface: GigabitEthernet2/0/0
        Upstream neighbor: 192.168.4.1
        RPF prime neighbor: 192.168.4.1
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet1/0/0
            Protocol: pim-sm, UpTime: 01:51:24, Expires: -

 (10.110.1.100, 225.1.1.1)
    RP: 10.10.1.1
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 01:51:24
    Upstream interface: GigabitEthernet2/0/0
        Upstream neighbor: 192.168.4.1
        RPF prime neighbor: 192.168.4.1
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet1/0/0
            Protocol: pim-sm, UpTime: 01:51:24, Expires: -
```

# 在RouterC上执行主备倒换命令:

```
[RouterC] slave switchover
Warning: Are you sure to switch over?[Y/N]:Y
```

# RouterC进行主备倒换后，在PIM GR期间，在RouterB和RouterC上分别使用**display pim routing-table**命令查看路由表，显示信息如下：

```
<RouterB> display pim routing-table
 VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 225.1.1.1)
    RP: 10.10.1.1
    Protocol: pim-sm, Flag: WC
    UpTime: 02:52:38
    Upstream interface: GigabitEthernet1/0/0
        Upstream neighbor: 192.168.2.1
        RPF prime neighbor: 192.168.2.1
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/0/0
            Protocol: pim-sm, UpTime: 02:52:38, Expires: 00:03:00

 (10.110.1.100, 225.1.1.1)
```

```
    RP: 10.10.1.1
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 02:52:38
    Upstream interface: GigabitEthernet1/0/0
        Upstream neighbor: 192.168.2.1
        RPF prime neighbor: 192.168.2.1
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/0/0
            Protocol: pim-sm, UpTime: 02:52:38, Expires: 00:03:12
<RouterC> display pim routing-table
 VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 225.1.1.1)
    RP: 10.10.1.1
    Protocol: pim-sm, Flag: WC
    UpTime: 02:51:24
    Upstream interface: GigabitEthernet2/0/0
        Upstream neighbor: 192.168.4.1
        RPF prime neighbor: 192.168.4.1
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet1/0/0
            Protocol: igmp, UpTime: 02:51:24, Expires: -

 (10.110.1.100, 225.1.1.1)
    RP: 10.10.1.1
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 02:51:24
    Upstream interface: GigabitEthernet2/0/0
        Upstream neighbor: 192.168.4.1
        RPF prime neighbor: 192.168.4.1
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet1/0/0
            Protocol: pim-sm, UpTime: 02:51:24, Expires: -
```

由以上显示信息可知，RouterC在主备倒换前后，其上游RouterB的下游接口没有变化。即RouterC在主备倒换后，使用备份的Join信息向上游发送加入消息，且在GR期间维持了组播转发表项，保证了GR期间组播数据的不间断转发。

在RouterC进行主备倒换后恢复组播路由表项的过程中，用户仍能够正常接收组播数据，业务未受到影响。

**----结束**

# 配置文件

- RouterA的配置文件

```
#
 sysname RouterA
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 10.110.1.1 255.255.255.0
 pim sm
#
interface LoopBack0
 ip address 10.10.1.1 255.255.255.255
 pim sm
#
```

```
ospf 1
 opaque-capability enable
 graceful-restart period 200
 area 0.0.0.0
  network 10.10.1.1 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
pim
 static-rp 10.10.1.1
#
return
```

- RouterB的配置文件

```
#
 sysname RouterB
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.2 24
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.4.1 24
 pim sm
#
ospf 1
 opaque-capability enable
 graceful-restart period 200
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
 static-rp 10.10.1.1
#
return
```

- RouterC的配置文件

```
#
 sysname RouterC
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.110.2.1 24
 pim sm
 igmp enable
#
interface GigabitEthernet2/0/0
 ip address 192.168.4.2 24
 pim sm
#
ospf 1
 opaque-capability enable
 graceful-restart period 200
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
 static-rp 10.10.1.1
 graceful-restart
 graceful-restart period 300
#
return
```

# 4.12 PIM（IPv4）常见配置错误

介绍常见配置错误及定位思路。

## 4.12.1 PIM-DM 网络无法正确建立 SPT

### 故障现象

PIM-DM网络配置完成后，用户主机通过IGMP协议向组播组G发出点播请求，无法收到组播数据。

### 操作步骤

**步骤1** 检查是否存在到达组播源的单播路由。

使用命令**display ip routing-table**查看设备有无到达组播源的单播路由表项。

组播路由依赖单播路由，如果没有，则需要通过配置单播路由协议动态生成或者静态配置到达组播源的单播路由表项。

**步骤2** 检查接口上是否使能PIM-DM，尤其是RPF接口上是否使能PIM-DM。

使用命令**display pim interface**查看接口上的PIM信息。

如果接口上没有显示信息，或者显示接口的模式为Sparse，表明PIM-DM没有使能，则需要在接口上执行命令**pim dm**使能PIM-DM。

**步骤3** 检查与用户主机网段直连的接口上是否使能IGMP。

使用命令**display igmp interface**查看与用户主机网段直连接口的IGMP信息。

如果接口上没有显示信息，则需要在接口上执行命令**igmp enable**使能IGMP。

**步骤4** 检查是否配置了source-policy。

在设备上执行**display current-configuration configuration pim**命令，查看PIM视图下的当前配置信息。

如果配置信息中出现“source-policy acl-number”或“source-policy acl-name”，则表明配置了源过滤规则。如果接收到的组播数据不在ACL允许的范围之内，则将被丢弃。建议执行**undo source-policy**命令删除该配置或重新配置ACL规则，确保用户需要的组播数据正常转发。

**----结束**

## 4.12.2 PIM-SM 网络中 RPT 无法正常转发数据

### 故障现象

为ASM提供服务的RPT建立不正常，用户主机不能接收到组播数据。

## 原因分析

本类故障的常见原因主要包括：

- 组播设备到RP的单播路由不通
- 各组播设备的RP地址不一致
- 组播设备的下游接口没有收到（*,G）加入
- 接口没有使能PIM-SM
- 到RP的RPF路由不正确（举例：单播路由环路）
- 配置问题（举例：MTU或组播边界配置不当等）

## 操作步骤

**步骤1** 检查PIM路由表中是否存在正确的（*,G）表项

在设备上执行**display pim routing-table** *group-address*命令，查看PIM路由表中是否存在到所需组播组G的（*,G）表项。

- 如果PIM路由表中的（*,G）表项存在且信息完全正确，则每隔15秒执行**display multicast forwarding-table** *group-address*命令，查看转发表中是否存在与（*,G）对应的（S,G）表项，并查看显示信息中的“Matched”计数是否保持增长。
  - 如果转发表中存在（S,G）表项且“Matched”计数保持增长，则表明上游设备到此设备的组播数据转发正常，但是由于某种原因导致无法向下游转发，可能是由于数据报文的TTL过小或转发问题。
  - 如果转发表中不存在（S,G）表项或“Matched”计数停止：
    - 如果当前设备不是RP，则表明当前设备没有收到组播数据，故障可能出在上游设备，请检查上游设备的PIM路由表中是否存在正确的（S,G）表项。
    - 如果当前设备已经是RP，则表明RPT已成功建立，但由于某种原因导致RP未收到组播源发出的组播数据。故障可能是由于源DR没有注册成功。
- 如果PIM路由表中不存在正确的（*,G）表项，请执行步骤2。

**步骤2** 检查上游设备的下游接口是否收到Join信息

在设备上执行**display pim control-message counters interface** *interface-type interface-number* **message-type join-prune**命令，查看下游接口收到的Join/Prune报文计数是否增加。

- 如果设备的下游接口收到的Join/Prune报文计数没有增加，在其下游邻居上执行**display pim control-message counters interface** *interface-type interface-number* **message-type join-prune**命令，查看下游是否向上游发出了Join/Prune报文。
  - 如果计数增加，则表明下游已经发出了Join/Prune报文，则PIM邻居间通信有问题。
  - 如果计数没有增加，则下游设备有问题，请排查下游设备的故障。
- 如果下游接口收到的Join/Prune报文计数增加，请执行步骤3。

**步骤3** 检查接口是否使能PIM-SM

以下接口未使能PIM-SM是常见的故障原因：

- 到达RP的RPF邻居接口

- 到达RP的RPF接口
- 直连用户主机网段的接口（组成员端DR的下游接口）

在设备上执行**display pim interface verbose**命令，查看接口的PIM信息。请重点检查上述接口是否使能PIM-SM。

- 如果在接口上使能PIM-SM时出现提示信息：“Error: Please enable multicast in the system view first.”，则首先在系统视图下使用**multicast routing-enable**命令使能组播功能。然后在接口上使能PIM-SM。
- 如果设备的所有接口均已使能PIM-SM，请执行步骤4。

**步骤4** 检查RP信息是否正确

在设备上执行**display pim rp-info**命令，查看设备是否已经学习到了为某组播组服务的RP信息，并且与其它所有设备为此组播组服务的RP信息一致。

- 如果设备上没有RP信息或RP信息与其他设备不同：
  - 如果网络中使用静态RP，请执行**static-rp**命令在所有设备上将为某组播组服务的RP地址配置为一致。
- 如果所有设备为某组播组服务的RP信息已保持一致，请执行步骤5。

**步骤5** 检查是否存在到达RP的RPF路由

在设备上执行**display multicast rpf-info** *source-address*命令，查看是否存在到达RP的RPF路由。

- 如果显示信息中不存在到RP的RPF路由，检查单播路由配置。请在设备与RP上分别执行**ping**命令，检查是否能够ping通对方。
- 如果显示信息中存在到RP的RPF路由：
  - 如果显示信息表明RPF路由为组播静态路由，执行**display current-configuration**命令查看组播静态路由配置是否合理。
  - 如果显示信息表明RPF路由为单播路由，执行**display ip routing-table**命令查看单播路由是否与RPF路由一致。
- 如果显示信息中存在到RP的RPF路由，且路由配置合理，请执行步骤6。

**步骤6** 检查转发组播数据的接口是否为组成员端DR

在设备上执行**display pim interface** *interface-type interface-number*命令，查看转发组播数据的接口是否为组成员端DR。

- 如果显示信息中没有local标记，请根据显示信息中的DR地址在DR设备上执行步骤7。
- 如果显示信息中有local标记，请执行步骤7。

**步骤7** 检查接口是否配置组播边界

在设备上执行**display current-configuration interface** *interface-type interface-number*命令，查看接口是否配置了组播边界。

- 如果某接口的配置信息中出现“multicast boundary”，表明该接口配置了组播边界。建议执行**undo multicast boundary** { *group-address* { *mask* | *mask-length* } | **all** }命令删除该配置或重新进行网络规划，确保RPF接口和RPF邻居接口没有配置组播边界。
- 如果接口没有配置组播边界，请执行步骤8。

**步骤8** 检查是否配置了source-policy

在设备上执行**display current-configuration configuration pim**命令，查看PIM视图下的当前配置信息。

- 如果配置信息中出现“source-policy acl-number”或“source-policy acl-name”，则表明配置了源过滤规则。如果接收到的组播数据不在ACL允许的范围之内，则将被丢弃。建议执行**undo source-policy**命令删除该配置或重新配置ACL规则，确保用户需要的组播数据正常转发。

**----结束**

## 4.12.3 PIM-SM 网络中 SPT 无法正常转发数据

### 故障现象

SPT建立不正常，用户主机不能接收到组播数据。

### 原因分析

本类故障的常见原因主要包括：

- 组播设备的下游接口没有收到（S,G）加入
- 接口没有使能PIM-SM
- 到组播源的RPF路由不正确（举例：单播路由环路）
- 配置问题（举例：MTU、切换阈值或组播边界配置不当等）

### 操作步骤

**步骤1** 检查PIM路由表中是否存在正确的（S,G）表项

在设备上执行**display pim routing-table**命令，查看PIM路由表中是否存在组播源S到达所需组播组G的（S,G）表项。

- 如果存在，但标志位为RPT，组播组属于ASM范围，上游接口是朝向RP的RPF接口，而不是到达组播源的SPT接口，则表明SPT没有成功建立。

  在组成员端DR上执行**display current-configuration configuration pim**命令，查看PIM视图下的当前配置信息。如果显示信息中出现“spt-switch-threshold traffic-rate”或“spt-switch-threshold infinity”，请执行**undo spt-switch-threshold**命令删除配置信息或执行**spt-switch-threshold** *traffic-rate*命令重新配置合理的traffic-rate。
- 如果存在，且标志位为SPT，请执行**display multicast forwarding-table**命令查看转发表中的（S,G）表项并且查看显示信息中的“Matched”计数是否保持增长。执行**display multicast forwarding-table**命令后，由于计数更新比较慢，请等待几分钟。
  - 如果“Matched”计数保持增长，则表明上游设备到当前设备的组播数据转发正常，但是由于某种原因导致组播数据无法向下游设备转发。
  - 如果“Matched”计数停止，当前设备不是源DR，表明当前设备没有收到组播数据，故障可能出在上游设备，请检查上游设备的PIM路由表中是否存在正确的（S,G）表项。
- 如果PIM路由表中不存在正确的（S,G）表项，请执行步骤2。

**步骤2** 检查下游接口是否收到Join信息

**说明**

如果当前设备是组成员端DR，请跳过此步骤。

下游接口发生故障，或者未使能PIM-SM协议，会造成收不到对应的（S,G）Join报文。

在设备上执行**display pim control-message counters interface** *interface-type interface-number* **message-type join-prune**命令，查看下游接口收到的Join/Prune报文计数是否增加。

- 如果下游接口收到的Join/Prune报文计数没有增加，在该接口对应的下游设备上执行**display pim control-message counters interface** *interface-type interface-number* **message-type join-prune**命令，查看下游是否向上游发出了Join/Prune报文。
  - 如果计数增加，表明下游已经发出了Join/Prune报文，则上下游PIM邻居间通信有问题。
  - 如果计数没有增加，则下游设备有问题，请排查下游设备的故障。
- 如果下游接口收到的Join/Prune报文计数增加，请执行步骤3。

**步骤3** 检查接口是否使能PIM-SM

到达组播源的RPF接口没有使能PIM-SM是常见的故障原因。

**说明**

部署PIM-SM网络时，建议在网络中所有设备上使能组播，在所有接口上使能PIM-SM协议。

在设备上执行**display pim interface verbose**命令，查看接口上的PIM信息。请重点查看上述接口是否配置PIM-SM。

- 如果显示信息中缺少设备的某接口信息或者某接口的PIM模式为Dense，请在该接口上配置**pim sm**。

  如果在接口上使能PIM-SM时出现提示信息：“Error: Please enable multicast in the system view first.”，请首先在系统视图下执行**multicast routing-enable**命令使能组播功能。然后在接口视图下执行**pim sm**命令使能PIM-SM。
- 如果设备的所有接口均已使能PIM-SM，请执行步骤4。

**步骤4** 检查是否存在到达组播源的RPF路由

在设备上执行**display multicast rpf-info** *source-address*命令，查看是否存在到达组播源的RPF路由。

- 如果显示信息中不存在到组播源的RPF路由，检查单播路由配置。建议在设备和组播源上分别执行**ping**命令，检查是否能够ping通对方。
- 如果显示信息中存在到组播源的RPF路由：
  - 如果显示信息表明RPF路由为组播静态路由，执行**display current-configuration**命令，查看组播静态路由配置是否合理。
  - 如果显示信息表明RPF路由为单播路由，执行**display ip routing-table**命令，查看单播路由是否与RPF路由一致。
- 如果显示信息中存在到组播源的RPF路由，且路由配置合理，请执行步骤5。

**步骤5** 检查转发组播数据的接口是否为组成员端DR

在设备上执行**display pim interface** *interface-type interface-number*命令，查看转发组播数据的接口是否为组成员端DR。

- 如果显示信息中没有local标记，请根据显示信息中的DR地址在DR设备上执行步骤6。
- 如果显示信息中有local标记，请执行步骤6。

**步骤6** 检查接口是否配置组播边界

在设备上执行**display current-configuration interface** *interface-type interface-number*命令，查看接口是否配置了组播边界。

- 如果某接口的配置信息中出现“multicast boundary”，表明该接口配置了组播边界。建议执行**undo multicast boundary** { *group-address* { *mask* | *mask-length* } | **all** } 命令删除该配置或重新进行网络规划，确保RPF接口和RPF邻居接口没有配置组播边界。
- 如果接口没有配置组播边界，请执行步骤7。

**步骤7** 检查是否配置了source-policy

在设备上执行**display current-configuration configuration pim**命令，查看PIM视图下的当前配置信息。

- 如果配置信息中出现“source-policy acl-number”或“source-policy acl-name”，则表明配置了源过滤规则。如果接收到的组播数据不在ACL允许的范围之内，则将被丢弃。建议执行**undo source-policy**命令删除该配置或重新配置ACL规则，确保用户需要的组播数据正常转发。

**----结束**

## 4.12.4 源 DR 在接收到组播数据报文后仍不向 RP 发送注册报文

### 故障现象

配置好组播网络后，组播源发送组播数据，发现RP没有生成表项，直连源的DR也没有向RP发送注册报文。

### 操作步骤

**步骤1** 在源DR上使用命令**display pim routing-table** *group-address*查看源DR是否认为自己是源DR。

只有是源DR的设备才会负责向RP注册。例如：

```
<Huawei> display pim routing-table 225.0.0.1
 VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry

 (172.16.0.12, 225.0.0.1)
     RP: 10.2.2.2
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 02:54:43
     Upstream interface: GigabitEthernet1/0/0
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/0
             Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
```

**步骤2** 如果没有**LOC**标记说明设备不认为自己是源DR，此时使用命令**display rm interface** *interface-type interface-number*查看入接口的Peer地址是否为组播源地址。

例如查看上一步骤中入接口GE1/0/0的Peer地址：

```
<Huawei> display rm interface gigabitethernet 1/0/0
Name: GigabitEthernet1/0/0
Physical IF Info:
 IfnetIndex: 0x6
 State: DOWN P2P MULT
 Hardware Address: 286E-D4D4-4F54
 Slot: 0(Logic Slot: 0)
 IntType: 3, PriLog: 0, MTU: 1500, Reference Count 1
 Bandwidth: 0, 64000
 Baudrate: 0, 64000
 Delay: 0, Reliability: 0, Load: 0
 LDP-ISIS sync capability: disabled
 LDP-OSPF sync capability: disabled
 InstanceID: 0, Instance Name: Public
 Age: 1236sec
Logical IF Info:
 IfnetIndex: 0x3E, PhyIndex: 21 Logical Index : 3,
 Dest: 172.16.0.12, Mask: 255.255.255.0
 State: UP PRM BCA MULT , Reference Count 3
 Age: 1623973sec
```

**步骤3** 由前两步骤如果发现组播源的地址不是该接口的Peer地址，将组播源地址改为该Peer地址后，源DR便可完成注册。

**----结束**

## 4.12.5 源 DR 向 RP 发送了注册报文之后，注册出接口一直存在

### 故障现象

配置好组播网络后，组播源发送组播数据到源DR。源DR将组播数据封装在注册报文中，向RP发送了注册报文之后，对应组播表项的注册出接口一直存在，源DR与RP之间没有建立起SPT。

### 原因分析

如果源DR没有收到RP发来的注册停止报文，源DR上相应组播表项的注册出接口就不会删除。导致这类问题的最常见原因就是源DR与RP之间单播路由异常。

### 操作步骤

**步骤1** 确认源DR和RP之间单播路由正确，且能够ping通。

- 如果源DR到RP的单播路由不存在或者存在但ping不通，那么会导致RP收不到注册报文，所以也就不会向源DR发送注册停止报文。
- 如果RP到源DR的单播路由不存在或者存在但ping不通，会导致RP发送给源DR的注册停止报文丢失。

**步骤2** 在RP上执行命令**display pim routing-table** *source-address*查看有无对应（S，G）表项。

如果单播能够ping通，再检查RP是否完成了到源方向的SPT切换，从而建立了一条到源DR的组播转发路径。如果RP到源方向的SPT切换尚未完成，RP不会发送注册停止报文。可能原因是RP到源端DR之间所有设备的接口上配置了不一致的PIM协议。

**----结束**

# 4.13 PIM（IPv4）FAQ

介绍配置过程中常见的问题，并给出相应的解答。

## 4.13.1 如何从配置上限制非法组播源

可以在PIM视图下，使用命令**source-policy** { *acl-number* | **acl-name** *acl-name* }来配置路由器对接收的组播数据报文根据源或源组进行过滤，从而达到限制非法组播源的目的。

# 4.14 PIM 参考信息

介绍PIM协议的相关RFC清单。

本特性的参考资料清单如下：

| 文档 | 描述 | 备注 |
| --- | --- | --- |
| RFC 4601 | Protocol Independent Multicast - Sparse Mode （PIM-SM） | - |
| RFC 5059 | Bootstrap Router （BSR） Mechanism for PIM | - |
| RFC 3973 | Protocol Independent Multicast - Dense Mode protocol | - |
| RFC 4607 | Source-Specific Multicast for IP | - |
| RFC 4610 | Anycast-RP Using Protocol Independent Multicast (PIM) | - |
| RFC 3569 | An Overview of Source-Specific Multicast (SSM) | - |
| RFC 4608 | Source-Specific Protocol Independent Multicast in 232/8 | - |
| RFC 3956 | Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address | - |