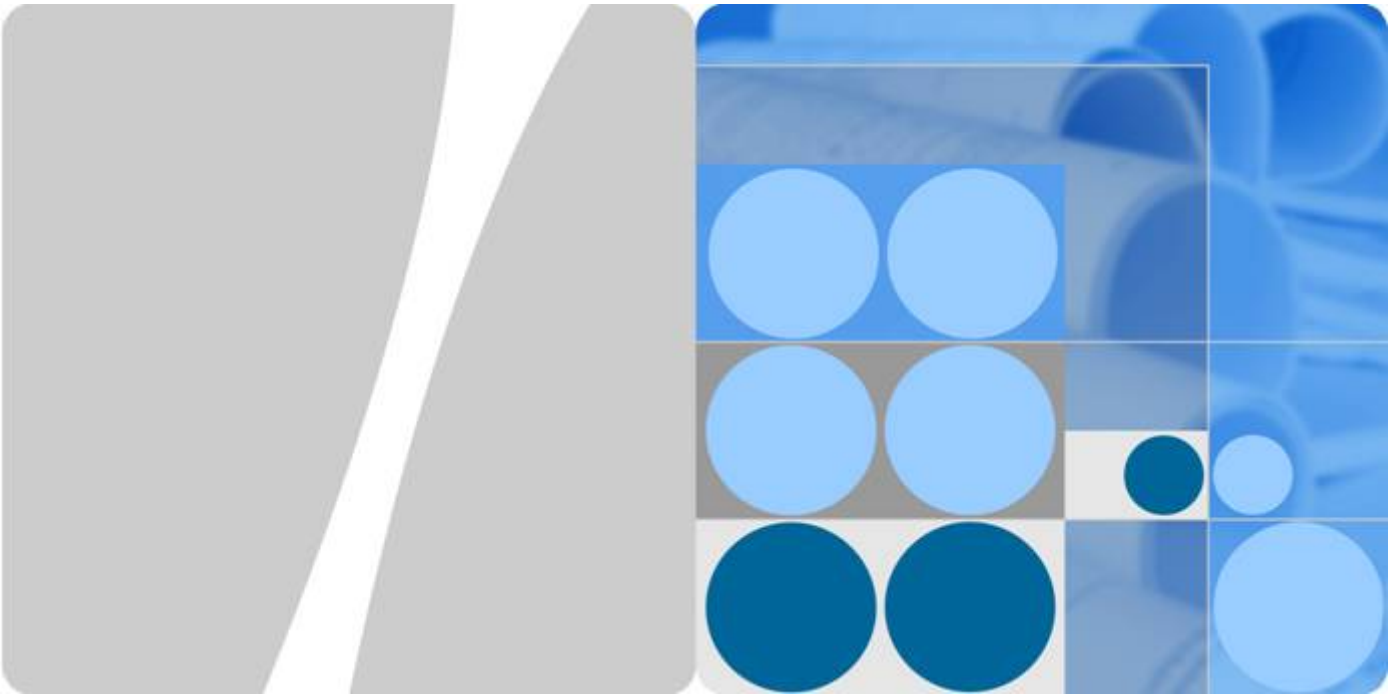


Huawei AR2200-S 系列企业路由器

V200R001C01

配置指南-组播

文档版本　01

发布日期　2012-01-06

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

读者对象

本文档介绍了 AR2200-S 中组播特性的基本概念、在不同应用场景中的配置过程和配置举例。

本文档提供了组播的配置方法。

本文档主要适用于以下工程师：

- 数据配置工程师
- 调测工程师
- 网络监控工程师
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
危险	以本标志开始的文本表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
警告	以本标志开始的文本表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。
说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

命令行格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... } *	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...] *	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复 1 ～ n 次。
#	由“#”开始的行表示为注释行。

接口编号约定

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

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2012-01-06)

第一次正式发布。

目 录

1 组播配置指导

关于本章

本章介绍组播的基本概念和相关协议、特性，并提供 IPv4 网络中典型的组播网络场景。

1.1 组播介绍
组播技术实现了网络中点到多点的高效数据传送，它能够有效地节约网络带宽、降低网络负载，所以在 IPTV、实时数据传送和多媒体会议等诸多方面都有广泛的应用。本节简要介绍组播出现的原因、优势以及组播在现实生活中的应用。

1.2 IPv4 组播相关概念
配置 IPv4 组播业务前，您将接触到组播基本概念、组播模型以及 IPv4 网络中的组播地址、组播协议。在了解这些概念和特性后，将对您配置组播业务有一定的帮助。

1.3 在 IPv4 网络中部署组播业务
介绍 IPv4 网络中几个典型的业务场景以及组播协议和特性在这些场景中的应用位置，帮助您更容易的配置组播业务。业务场景包括 PIM 域内、PIM-SM 域间和 AS 域间的应用。

1.1 组播介绍

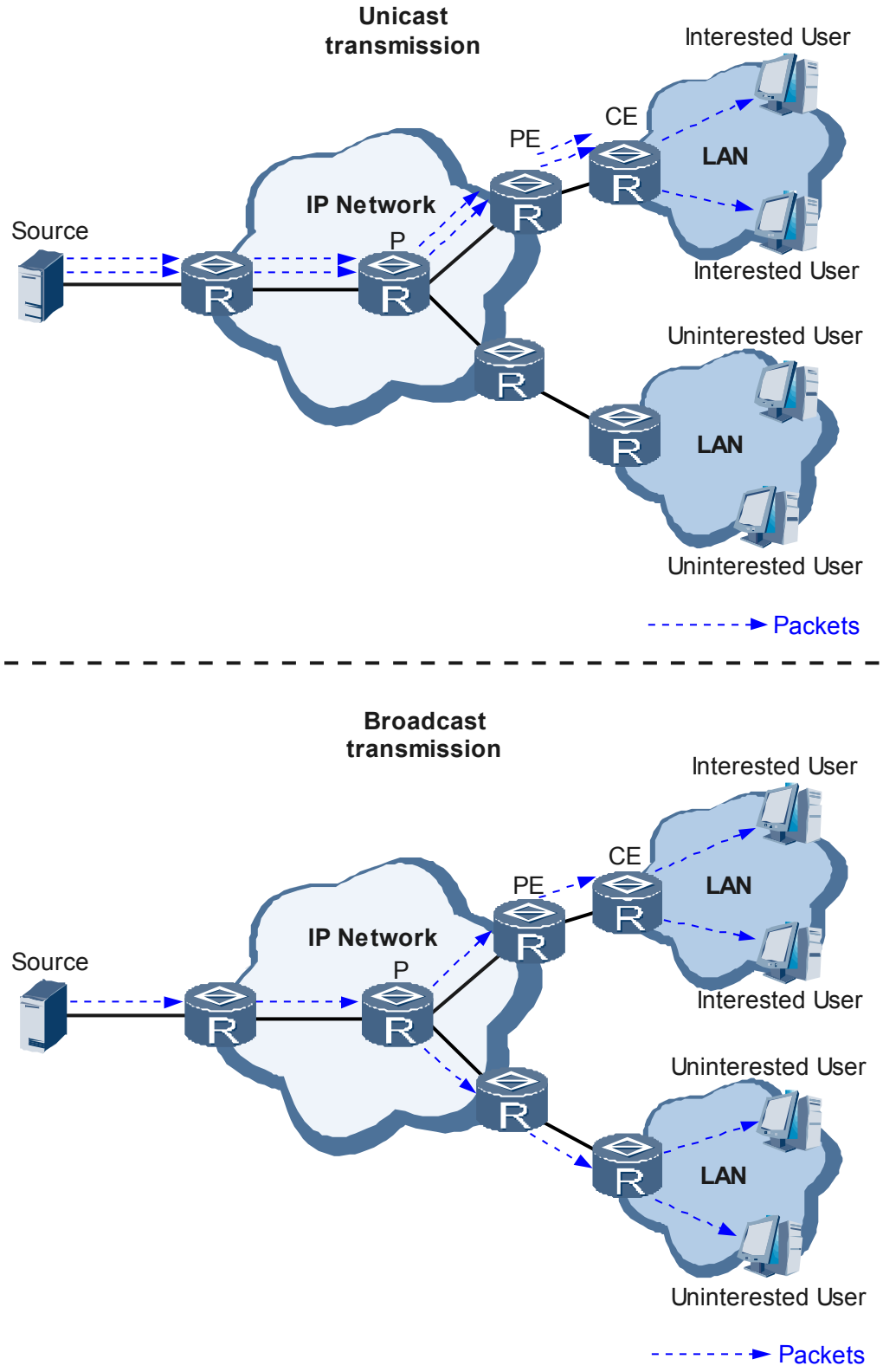
组播技术实现了网络中点到多点的高效数据传送，它能够有效地节约网络带宽、降低网络负载，所以在 IPTV、实时数据传送和多媒体会议等诸多方面都有广泛的应用。本节简要介绍组播出现的原因、优势以及组播在现实生活中的应用。

组播产生原因

传统的 IP 通信有两种方式：单播（Unicast），即数据从一台源 IP 主机传输到一台目的 IP 主机；广播（Broadcast），即数据从一台源 IP 主机向本网段中所有其它的 IP 主机发送。

如果要将数据从一台主机发送给多个主机而非所有主机，则要么采用广播方式，要么由源主机分别向网络中的多台目标主机以单播方式发送多份数据，如图 1-1 所示：

图 1-1 采用单播和广播方式进行点对多点传输数据示意图



- 采用单播方式实现时，传输信息量与需要该信息的用户量成正比，因此当需要该信息的用户数量较大时，信息源 Source 需要将多份内容相同的信息发送给不同的用

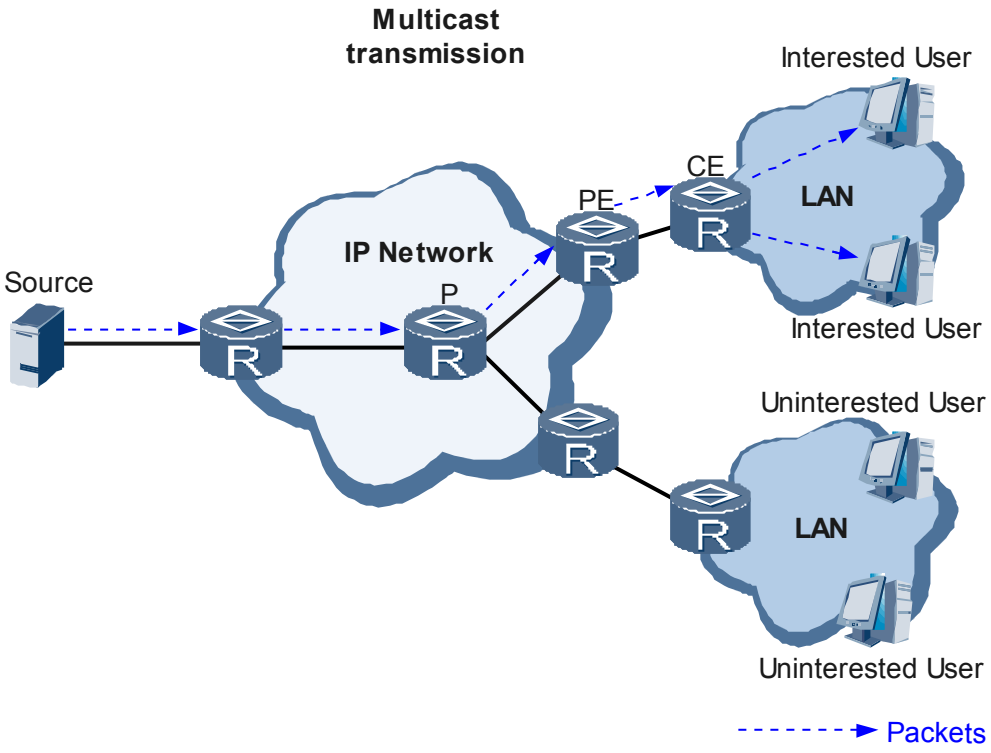
户 Host，这对信息源 Source 以及从 Source 到 CE 带宽都将造成巨大的压力。由此可以看出，该传输方式不利于信息的批量发送。

- 采用广播方式实现时，不需要信息的 Uninterested User 也将收到该信息，这样不仅信息的安全性得不到保障，而且会造成 P 到 CE 的信息泛滥。由此可见，该传输方式不利于与特定对象进行数据交互，并且还浪费了大量的带宽。

由上述可见，传统的单播和广播通信方式不能有效地解决单点发送、多点接收的问题。

组播（multicast）可以很好的解决点对多点的数据传输，如图 1-2 所示，源 Source 只发送一份数据，所有接收者都可接收到同样的数据拷贝，并且只有需要该数据的主机（目标主机）可以接收该数据，网络中其它主机不能收到该数据。在数据传输的同时，组播能够保障信息的安全性且只占用有限的网络带宽。

图 1-2 采用组播方式进行点对多点传输数据示意图



组播优势

组播不同于单播和广播，它既不指定明确的接收者，也不是将数据分发给网络上的所有主机。组播相对单播和广播有如下优势：

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

应用

组播技术有效地解决了单点发送、多点接收的问题，实现了 IP 网络中点到多点的高效数据传送，能够大量节约网络带宽、降低网络负载。更重要的是，组播利用网络的组播特性方便地提供一些新的增值业务来实现的互联网信息服务，包括在线直播、网络电视、远程教育、远程医疗、网络电台、实时视频会议等互联网的信息服务领域，可以更加丰富人们的沟通与生活。

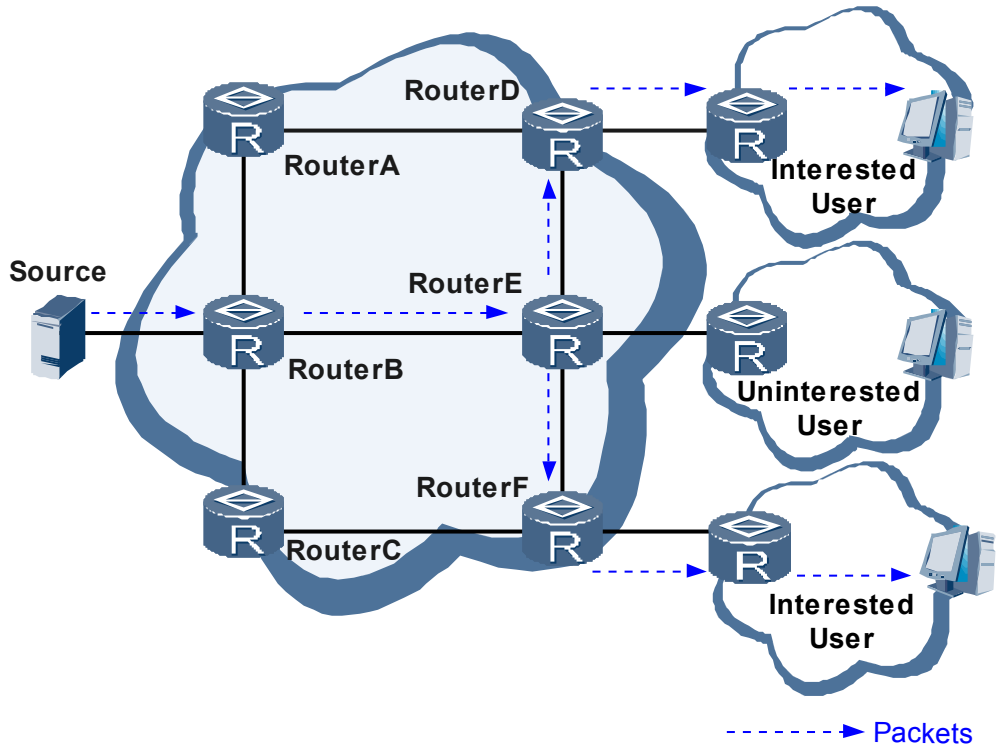
1.2 IPv4 组播相关概念

配置 IPv4 组播业务前，您将接触到组播基本概念、组播模型以及 IPv4 网络中的组播地址、组播协议。在了解这些概念和特性后，将对您配置组播业务有一定的帮助。

组播中的基本概念

如图 1-3 所示，网络中存在信息发送者 Source，Interested User 提出信息需求，网络采用组播方式传输信息。

图 1-3 组播方式示意图



- 组播组：用 IP 组播地址进行标识的接收者集合，主机通过加入某组播组，从而可以接收发往该组播组的组播数据。
- 组播源：信息的发送者称为“组播源”，如图 1-3 中的 Source。一个组播源可以同时向多个组播组发送信息，多个组播源也可以同时向一个组播组发送信息。组播源通常不需要加入组播组。

- 组播组成员：所有加入某组播组的主机便成为该组播组的成员，如图 1-3 中的Interested User。组播组中的成员是动态的，主机可以在任何时刻加入或离开组播组。组播组成员可以广泛地分布在网络中的任何地方。
- 组播路由器：支持三层组播功能的路由器或三层交换机，图 1-3 中的各个 Router。组播路由器不仅能够提供组播路由功能，也能够在与用户连接的末梢网段上提供组播组成员的管理功能。组播路由器本身也可能是组播组的成员。

组播模型

根据接收者对组播源处理方式的不同，组播模型分为以下两类：

- ASM（Any-Source Multicast）任意源组播模型

  在 ASM 模型中，任意一个发送者都可以作为组播源向某组播组地址发送信息，众多接收者通过加入由该组播组地址标识的组播组以获得发往该组播组的组播信息。接收者无法预先知道组播源的位置，但可以在任意时间加入或离开该组播组。
- SSM（Source-Specific Multicast）指定信源组播模型

  有些情况下，用户只对某些组播源发送的组播信息感兴趣，而不愿接收其它源发送的信息，SSM 模型就为用户提供了这样一种能够在客户端指定组播源的传输服务。SSM 模型中的接收者已经通过其它手段预先知道了组播源的具体位置，可以直接在接收者与其指定的组播源之间建立专用的组播转发路径。

而且为了便于接受者进行区分，SSM 模型与 ASM 模型使用不同的组播地址范围。

IPv4 组播地址

在基于 IPv4 的网络中，为了让组播源和组播组成员进行通信，需要提供网络层组播地址，即 IPv4 组播地址。任何用户主机（或其他接收设备）加入此范围内的某组播组，就成为了该组成员，可以识别并接收以该组播地址为目的地址的 IP 报文。网络中的组成员可能广泛分布在网络中的任何地方，用户主机可以在任何时刻加入或者离开组播组。IPv4 组播地址使用 D 类地址，其范围是：224.0.0.0 ～ 239.255.255.255。各地址段含义见表 1-1。

表 1-1 IPv4 组播地址的范围及含义

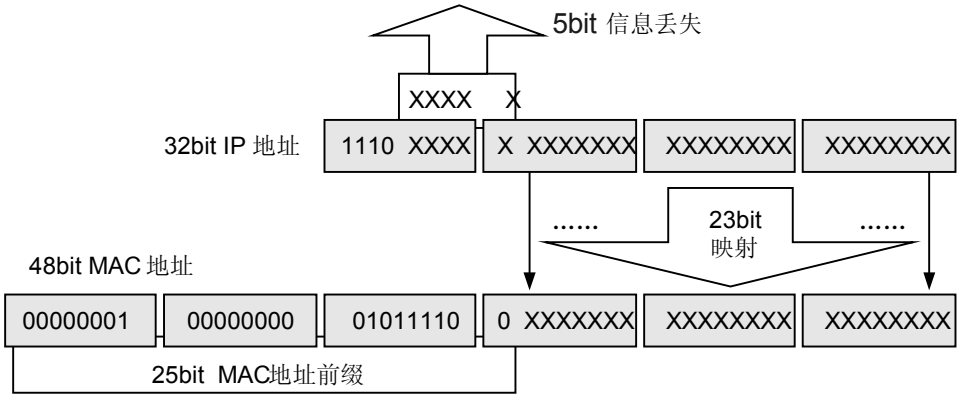
D 类地址范围	含义
224.0.0.0 ～ 224.0.0.255	本地链路的保留组地址。IANA 为路由协议预留的组播地址（也称为永久组地址），用于标识一组特定的网络设备，不用于组播转发。
224.0.1.0 ～ 231.255.255.255 233.0.0.0 ～ 238.255.255.255	ASM 组播地址，全网范围内有效。
232.0.0.0 ～ 232.255.255.255	缺省情况下的 SSM 组播地址，全网范围内有效。
239.0.0.0 ～ 239.255.255.255	管理范围组地址。缺省的 BSR 管理域组地址范围，仅在 BSR 管理域内有效，属于私有地址。在不同的 BSR 管理域内使用相同的地址不会冲突。

IPv4 组播 MAC 地址

以太网传输 IPv4 单播报文的时候，目的 MAC 地址使用的是接收者的 MAC 地址。但是在传输组播数据包时，其目的地不再是一个具体的接收者，而是一个成员不确定的组，所以要使用IPv4 组播 MAC 地址，即 IPv4 组播地址映射到链路层中的地址。

IANA 规定，IPv4 组播 MAC 地址的高 24bit 为 0x01005e，第 25bit 为 0，低 23bit 为 IPv4 组播地址的低 23bit，映射关系如图 1-4 所示。例如某组播组的 IPv4 组播地址为 224.0.1.1，则该组播组的 IPv4 组播 MAC 地址为 01-00-5e-00-01-01。

图 1-4 IPv4 组播地址与 IPv4 组播 MAC 地址的映射关系



由于 IPv4 组播地址的前 4bit 是 1110，代表组播标识，但是后 28bit 中只有 23bit 被映射到 MAC 地址，这样 IP 地址中就有 5bit 信息丢失，直接的结果是出现了 32 个 IPv4 组播地址映射到同一 MAC 地址上，当按 MAC 地址转发时，如果发生地址冲突，请将配置修改成按 IP 地址转发组播数据。例如组播 IP 地址为 224.0.1.1、224.128.1.1、225.0.1.1、239.128.1.1 等组播组的组播 MAC 地址都为 01-00-5e-00-01-01。

IPv4 组播协议

表 1-2 IPv4 组播协议

协议	功能	备注
PIM（Protocol Independent Multicast）协议无关组播	PIM 作为一种 IPv4 网络中的组播路由协议，主要用于将网络中的组播数据流发送到有组播数据请求的组成员所连接的路由器上，从而实现组播数据流的路由查找与转发。PIM 协议包括适合网络规模较大、组成员相对比较分散的 PIM-SM（Protocol Independent Multicast Sparse Mode）协议无关组播-稀疏模式和适合网络规模较小、组播组成员相对比较集中的 PIM-DM（Protocol Independent Multicast Dense Mode）协议无关组播－密集模式。	在 PIM-DM 模式下不需要区分 ASM 模型和 SSM 模型。 在 PIM-SM 模式下根据数据和协议报文中的组播地址区分 ASM 模型和 SSM 模型： ● 如果在 SSM 组播地址范围内，则构建 PIM-SM 在 SSM 中的实现模式。PIM-SSM 不但效率高，而且简化了组播地址分配流程，特别适用于对于特定组只有一个特定源的情况。 ● 如果在 ASM 组播地址范围内，则按照 PIM-SM 在 ASM 中的实现流程进行处理。 请参见 **4.1 PIM-DM 概述** 和 **5.1 PIM-SM 概述**。
IGMP（Internet Group Management Protocol）组播组管理协议	IGMP 是负责 IPv4 组播成员管理的协议，运行在组播网络中的最后一段，即组播网络中三层网络设备与用户主机相连的网段内。IGMP 协议在主机端实现组播组成员加入与离开，在上游的三层设备中实现组成员关系的维护与管理，同时支持与上层组播路由协议的信息交互。	到目前为止，IGMP 有三个版本：IGMPv1 版本、IGMPv2 版本和 IGMPv3 版本。 所有 IGMP 版本都支持 ASM 模型。IGMPv3 可以直接应用于 SSM 模型，而 IGMPv1 和 IGMPv2 则需要 SSM Mapping 技术的支持。 请参见 **3.1 IGMP 概述**。
MSDP（Multicast Source Discovery Protocol）组播源发现协议	MSDP 是为了解决多个 PIM-SM 域之间的互连的一种域间组播协议，用来发现其它 PIM-SM 域内的组播源信息，将远端域内的活动信源信息传递给本地域内的接受者，从而实现组播报文的跨域转发。	在 PIM-SM 模式在使用 SSM 模型的情况下不需要使用 MSDP。 请参见 **6.1 MSDP 概述**。

协议	功能	备注
MBGP（MultiProtocol Border Gateway Protocol）组播边界网关协议	MBGP 是 MP-BGP（Multi-Protocol BGP，多协议 BGP）在组播上的应用协议，实现组播源与组播接收者跨 AS 域进行组播转发。	
IPv4 组播路由管理	IPv4 组播路由管理用于管理组播路由表，能够控制组播路由创建或改变组播路由。	请参见 **7.1 IPv4 组播路由管理概述**。

1.3 在 IPv4 网络中部署组播业务

介绍 IPv4 网络中几个典型的业务场景以及组播协议和特性在这些场景中的应用位置，帮助您更容易的配置组播业务。业务场景包括 PIM 域内、PIM-SM 域间和 AS 域间的应用。

注意

请务必根据网络实际情况和具体的业务需求，有针对性的定制配置方案。本节仅介绍基本业务功能的部署。

说明

部署 IPv4 组播业务前，首先确保网络中 IPv4 单播路由正常。

- 在一个小型局域网中，所有的设备和主机都在一个 PIM 组播域内，此时的组播业务基本部署如**图 1-5** 和**表 1-3** 所示。

图 1-5 PIM 域内组播业务的基本部署示意图

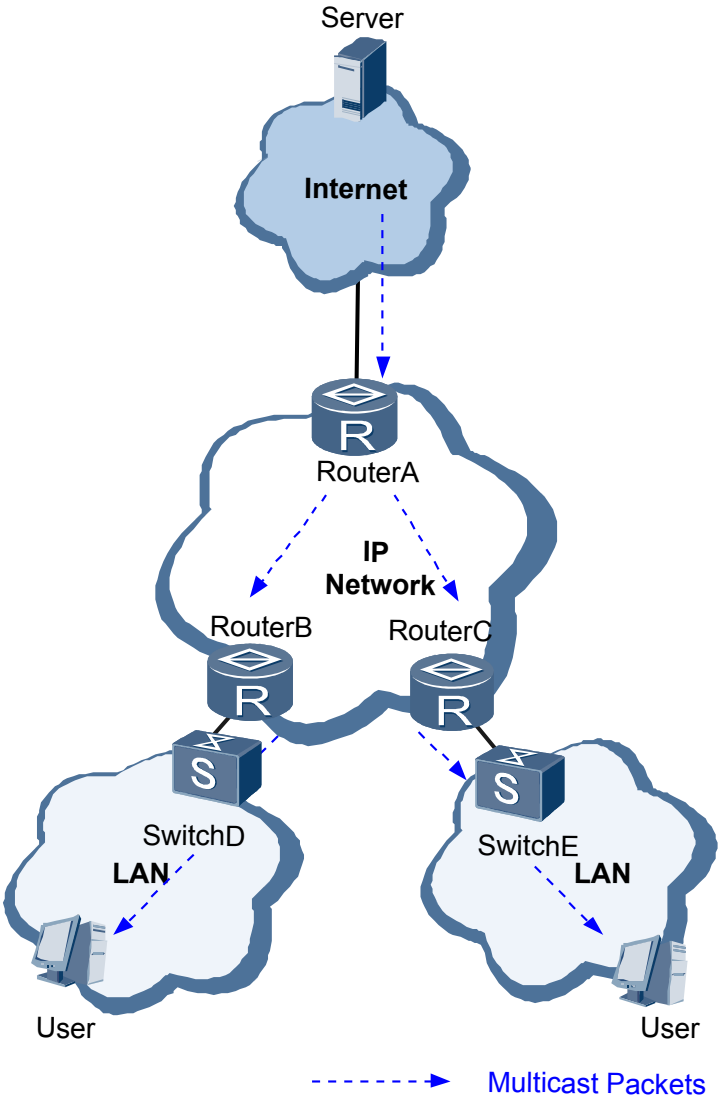


表 1-3 PIM 域内组播业务的各设备应用组播协议

部署协议	应用位置	目的
PIM （必选）	在组播域内的路由器所有接口，包括： ● RouterA 的所有接口 ● RouterB 的所有接口 ● RouterC 的所有接口 具体配置请参见 **4 PIM-DM（IPv4）配置**和 **5 PIM-SM（IPv4）配置**。	将组播数据流从组播源 Server 发送到与有组播需求的用户相连的 RouterB 和 RouterC 上。

部署协议	应用位置	目的
IGMP （必选）	在组播路由器与用户连接侧： ● RouterB 的用户侧接口 ● RouterC 的用户侧接口 具体配置请参见 **3 IGMP 配置**。	实现组播组成员 User 加入与离开组播组，RouterB 和 RouterC 维护与管理组成员。
IGMP Snooping （必选）	在用户主机与组播路由器之间的二层设备： ● RouterD 的 VLAN 内 ● RouterE 的 VLAN 内 具体配置请参见 **2.3 配置基于 VLAN 的 IGMP Snooping**。	侦听 RouterC 和 User 之间发送的 IGMP 消息建立组播数据报文的二层转发表，从而管理和控制组播数据报文在二层网络中的转发。

- 为了对组播资源（组播组、组播源和组播成员）便于控制和管理，运营商往往对组播资源在域间进行隔离，从而形成一个个隔离的 PIM-SM 域。但是如果需要不同的 PIM-SM 域之间组播数据互通，就需要部署 MSDP 协议，如**图 1-6** 和**表 1-4** 所示。

  说明

  PIM-SM 模式在使用 SSM 模型的情况下不需要使用 MSDP 协议。

图 1-6 跨 PIM-SM 域组播业务的基本部署示意图

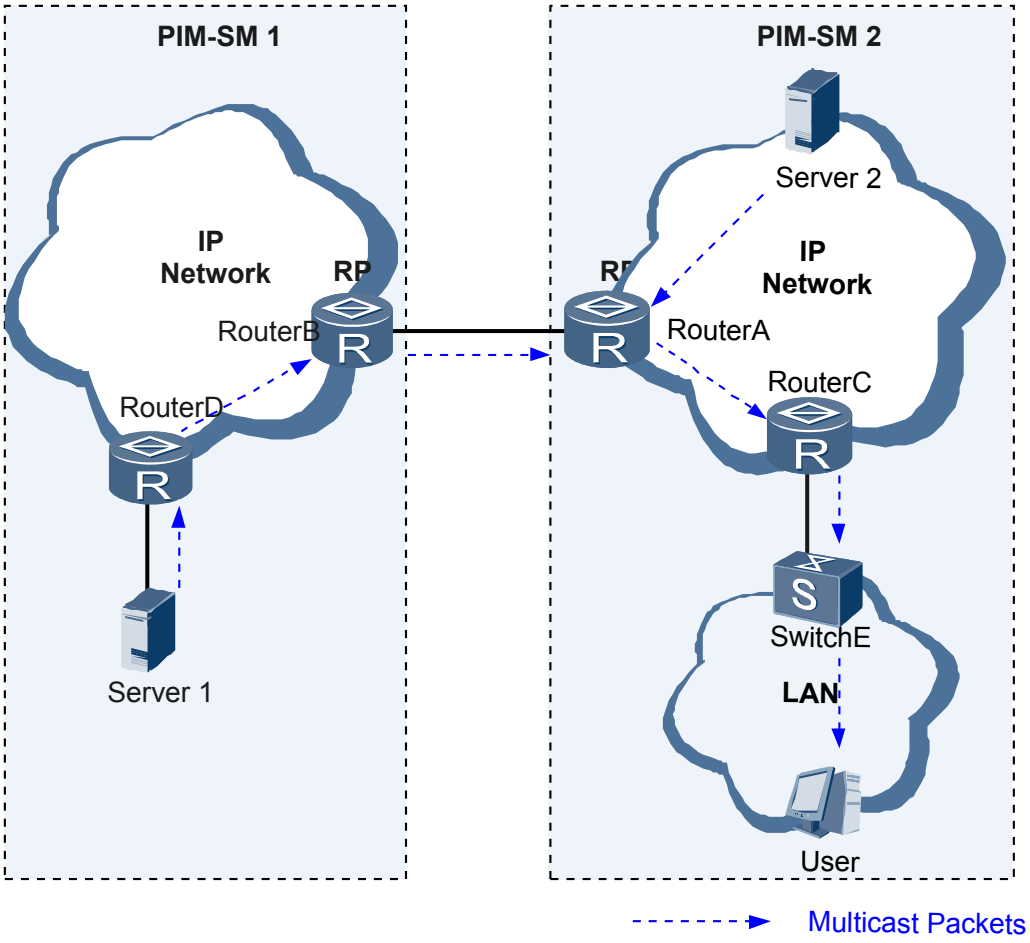


表 1-4 跨 PIM-SM 域业务的各设备应用组播协议

部署协议	应用位置	目的
PIM-SM （必选）	在各 PIM-SM 域内组播路由器的所有接口，包括： ● RouterA 的所有接口 ● RouterB 的所有接口 ● RouterC 的所有接口 ● RouterD 的所有接口 具体配置请参见 **5 PIM-SM（IPv4）配置**。	将组播数据流从组播源 Server1 和 Server2 发送到与有组播需求的用户相连的 RouterC 上。PIM-SM 采用接收者 User 主动加入组播组、然后组播数据通过汇聚点 RP 发送信息到接受者的方式完成组播传输。
IGMP （必选）	在各 PIM-SM 域内组播路由器与用户连接侧： ● RouterC 的用户侧接口 具体配置请参见 **3 IGMP 配置**。	实现组播组成员 User 加入与离开组播组，RouterC 维护与管理组成员。

部署协议	应用位置	目的
MSDP （必选）	在需要互连的各个 PIM-SM 域中的汇聚点 RP，包括： ● RouterA ● RouterB 具体配置请参见 6 MSDP 配置。	实现组播源信息在 PIM-SM1 和 PIM-SM2 域间传递。

- 由于 PIM 协议依赖于单播路由表，从而组播转发路径与单播转发路径是一致的。实际上，运营商希望 AS（Autonomous System）域间的组播转发路径独立于单播路径，并且能够进行有效控制。此时可以部署 MBGP 协议，生成一张独立于单播路由的组播路由表，使组播数据通过组播路由表进行传输，如图 1-7 和表 1-5 所示。

  说明

  跨 AS 域部署 MBGP 协议前，首先部署 AS 域间的 BGP 功能。

图 1-7 跨 AS 域组播业务的基本部署示意图

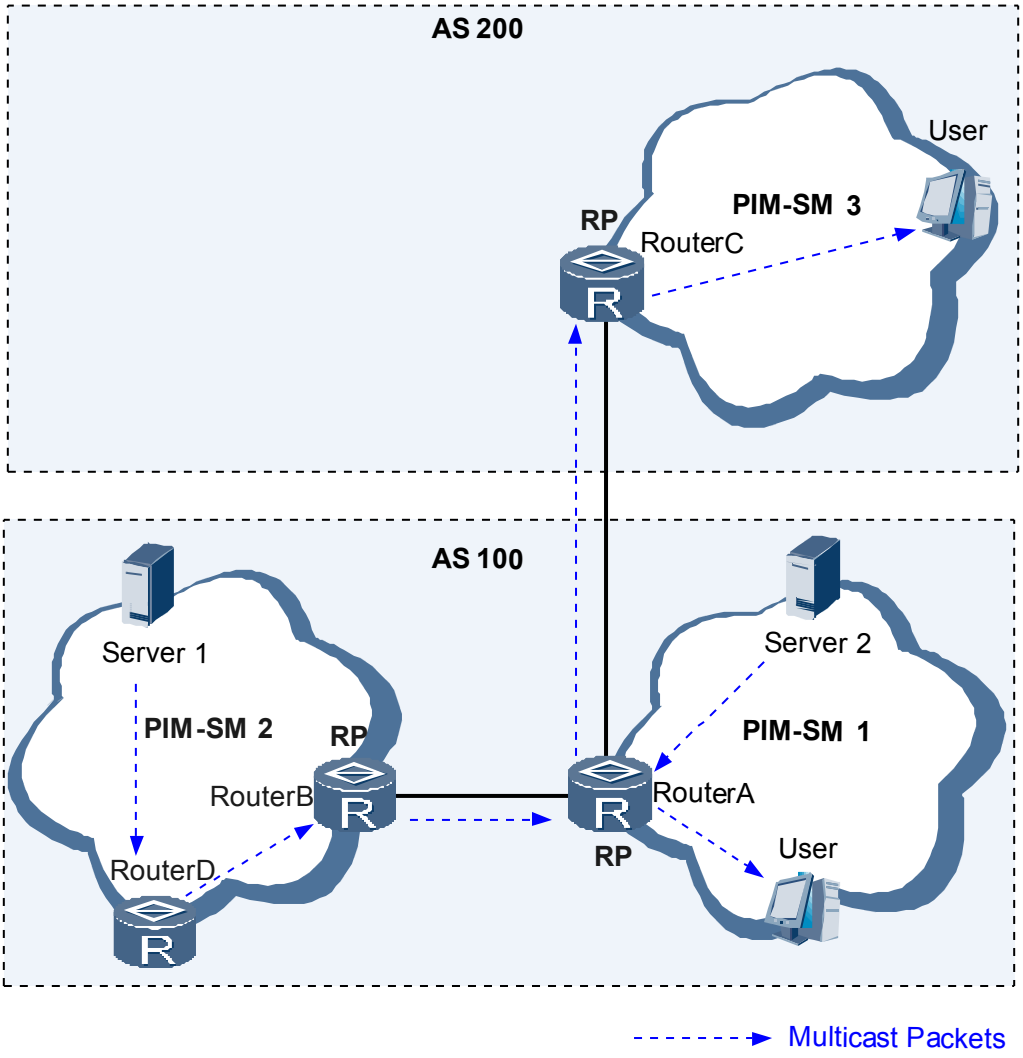


表 1-5 跨 AS 域业务的各设备应用组播协议

部署协议	应用位置	目的
PIM-SM （必选）	在各 PIM-SM 域内组播路由器的所有接口，包括： ● RouterA 的所有接口 ● RouterB 的所有接口 ● RouterC 的所有接口 ● RouterD 的所有接口 具体配置请参见 **5 PIM-SM（IPv4）配置**。	将组播数据流从组播源 Server1 和 Server2 发送到与有组播需求的用户相连的 RouterA 和 RouterC 上。PIM-SM 采用接收者 User 主动加入组播组、然后组播数据通过汇聚点 RP 发送信息到接受者的方式完成组播传输。
IGMP （必选）	在各 PIM-SM 域内组播路由器与用户连接侧： ● RouterA 的用户侧接口 ● RouterC 的用户侧接口 具体配置请参见 **3 IGMP 配置**。	实现组播组成员 User 加入与离开组播组，RouterA 和 RouterC 维护与管理组成员。
MSDP （必选）	在需要互连的各个 PIM-SM 域中的 RP，包括： ● RouterA ● RouterB ● RouterC 具体配置请参见 **6 MSDP 配置**。	实现组播源信息在 PIM-SM1 和 PIM-SM2 以及 PIM-SM1 和 PIM-SM3 域间传递。

2 IGMP Snooping 配置

关于本章

介绍 IGMP Snooping 特性的配置方法和维护命令，并提供配置举例。

2.1 IGMP Snooping 概述
介绍 IGMP Snooping 协议的功能和优势。

2.2 AR2200-S 支持的 IGMP Snooping 特性
介绍 IGMP Snooping 特性在 AR2200-S 中的支持情况。

2.3 配置基于 VLAN 的 IGMP Snooping
介绍如何配置基于 VLAN 的 IGMP Snooping。

2.4 配置 IGMP Snooping 的 SSM Mapping 功能
介绍 IGMP Snooping 的 SSM Mapping 功能的配置方法。

2.5 维护
清除 IGMP Snooping 的统计数据。

2.6 配置举例
介绍 IGMP Snooping 的配置举例。

2.1 IGMP Snooping 概述

介绍 IGMP Snooping 协议的功能和优势。

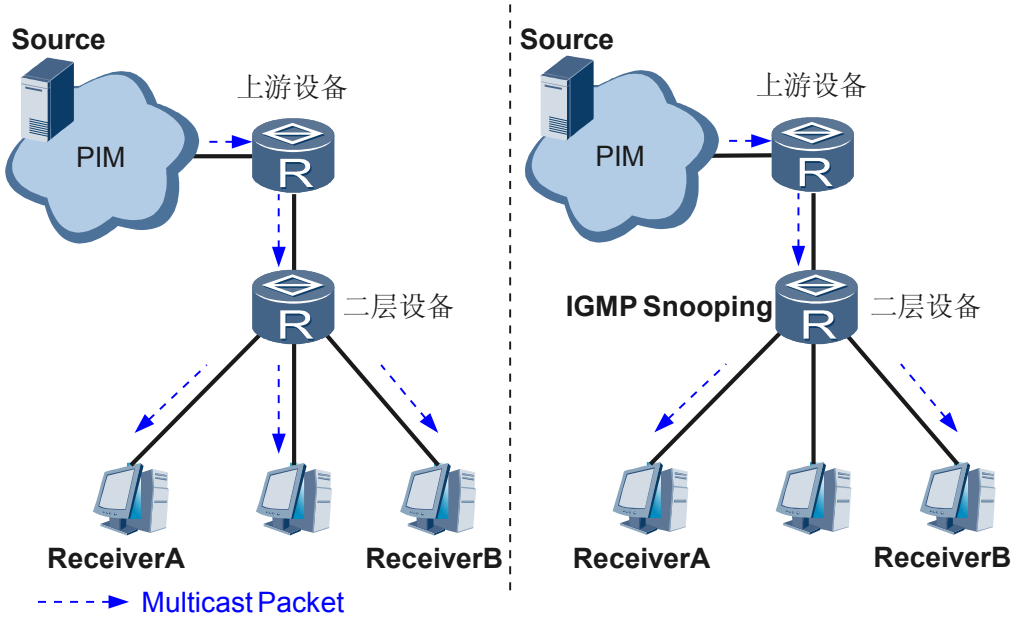
IGMP Snooping 功能

IGMP Snooping(Internet Group Management Protocol Snooping)是一种二层组播协议，通过侦听上层路由器和用户主机之间发送的组播协议报文来维护组播报文的出端口信息，从而管理和控制组播数据报文的转发。

在网络运行环境中，当上游设备将组播报文转发下来以后，处于接入边缘的设备负责将组播报文转发给组播用户，使用户收看所点播的节目。如图 2-1 所示，缺省情况下，组播数据在数据链路层被广播，造成带宽浪费，并使付费和未付费用户都能收看所点播的节目。

在二层设备上配置 IGMP Snooping 后，已知组播组的组播数据不会在数据链路层被广播，而会发给指定的接收者，使只有付费的用户才能收看所点播的节目。

图 2-1 二层设备运行 IGMP Snooping 前后的对比



IGMP Snooping 优势

IGMP Snooping 通过二层组播将信息只转发给有需要的接收者，有以下优点：

- 减少了二层网络中的广播报文，节约带宽
- 增强了组播信息的安全性
- 为实现每台用户主机的单独计费提供了方便

2.2 AR2200-S 支持的 IGMP Snooping 特性

介绍 IGMP Snooping 特性在 AR2200-S 中的支持情况。

IGMP Snooping

AR2200-S 支持配置基于 VLAN 的 IGMP Snooping 功能。

IGMP Snooping 通过侦听上层路由器和主机之间发送的组播协议报文来维护组播报文的出端口信息，从而管理和控制组播数据报文的转发，实现二层组播。

通过配置成员接口静态加入组播组，实现用户长期稳定接收组播数据报文。

当二层网络变化时，配置主动发送 IGMP Query 报文，使 AR2200-S 感知二层网络拓扑变化，按照新的网络拓扑正确转发组播数据，从而保证业务不间断。

端口快速离开

端口快速离开是指当 AR2200-S 某端口收到主机发送的离开某指定组播组的 IGMP Leave 消息时，就将该端口从指定组播组的出端口信息中删除。在组播应用于 IPTV 的场景下，需要配置端口快速离开机制， 在这种场景中 AR2200-S 端口一般只连接一个用户主机，快速离开可以保证用户切换频道的速度。

IGMP Snooping 端口快速离开有以下优点：

- 减小响应延迟。
- 节省因各种消息而占用的网络带宽。

IGMP Snooping 查询器

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

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

IGMP Snooping 策略

根据需要配置不同 IGMP Snooping 策略。

- 允许接口加入的组播组最大数量，限制用户点播组播节目的数量，控制接口上的数据流量。
- 组播组过滤器的配置，限制用户对组播节目的点播。
- IGMP 报文抑制，只会转发第一个 IGMP 成员关系报告报文（Report 和 Leave 报文），减少网络中报文的数量。
- 对于组播业务比较稳定的网络，比如说静态二层组播业务，对于未知组播报文可以无需处理；对于组播业务不太稳定，有组播用户频繁加入和退出的情况，对于未知组播报文必须进行处理，否则可能会导致部分用户无法接收到组播数据。

IGMP Snooping SSM Mapping 功能

SSM 模型中，如果接收者主机上运行的是 IGMPv3，则可以在 IGMPv3 的组播数据报文中直接指定组播源的地址；如果某些接收者主机只能运行 IGMPv1 或 IGMPv2，则在 IGMPv1 或 IGMPv2 的组播数据报文中无法指定组播源的地址。配置 IGMP Snooping SSM Mapping 功能，可以使组播组与组播源之间能够建立一一对应的映射关系，将 IGMPv1 或 IGMPv2 数据报文中所包含的（*,G）信息映射为(S,G)信息，提供 SSM 组播服务。

2.3 配置基于 VLAN 的 IGMP Snooping

介绍如何配置基于 VLAN 的 IGMP Snooping。

2.3.1 建立配置任务

应用环境

基于 VLAN 的 IGMP Snooping 运行在位于路由器和用户主机之间的 AR2200-S 上，通过侦听上层路由器和主机之间发送的组播协议报文来维护组播报文的转发表项，从而管理和控制组播数据报文的转发，实现二层组播。

前置任务

在配置基于 VLAN 的 IGMP Snooping 功能之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 创建 VLAN，接口加入 VLAN。

数据准备

在配置基于 VLAN 的 IGMP Snooping 功能之前，需要准备以下数据。

序号	数据
1	配置 IGMP Snooping 的 VLAN 编号
2	（可选）IGMP Snooping 可以处理 IGMP 报文的版本号
3	相关功能的接口类型和编号
4	（可选）查询器的参数：通用查询时间间隔、健壮系数、最大响应时间和最后成员查询时间间隔
5	路由器接口老化时间
6	IGMP 查询报文的源 IP 地址

2.3.2 配置 IGMP Snooping 基本功能

背景信息

缺省情况下 AR2200-S 的 IGMP Snooping 功能处于关闭状态，因此需要使能全局 IGMP Snooping 功能，再使能 VLAN 内 IGMP Snooping 功能。

如果 AR2200-S 需要对不同版本的 IGMP 报文进行处理，可以配置 IGMP Snooping 的版本。

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 **igmp-snooping enable**，使能全局 IGMP Snooping 功能。

步骤 3 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 4 执行命令 **igmp-snooping enable**，使能 VLAN 的 IGMP Snooping 功能。

说明

在 VLAN 内使能 IGMP Snooping 之前，必须先在系统视图下全局使能 IGMP Snooping，否则将无法在 VLAN 内使能 IGMP Snooping。

步骤 5 （可选）执行命令 **igmp-snooping version** *version*，配置 IGMP Snooping 可以处理的 IGMP 版本。

说明

当 IGMP Snooping 的版本为 1 时，IGMP Snooping 只能够对 IGMPv1 报文进行处理。

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

当 IGMP Snooping 的版本为 3 时，IGMP Snooping 能够对 IGMPv1、IGMPv2 和 IGMPv3 的报文进行处理。

----结束

2.3.3 （可选）配置路由器接口功能

背景信息

路由器接口用来接收上游设备的组播数据报文，缺省情况下为动态路由器接口。当网络发生拥塞或者网络稳定性不佳，动态路由器接口在其老化时间超时前没有收到 IGMP 普遍组查询报文或者 PIM Hello 报文，设备将把该接口从路由器接口列表中删除，造成组播数据中断，因此需要将路由器接口老化时间值适当调大。如果需要长期稳定接收组播数据报文，可以配置静态路由器接口，接口不会老化，从而避免组播业务中断。

VLAN 内当不需要动态路由器接口接收组播数据报文，可以配置禁止使能路由器接口学习功能，则 VLAN 内路由器接口只能手工配置成静态路由器接口。

操作步骤

- 配置动态路由器接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。

3. 执行命令 **igmp-snooping router-aging-time** *router-aging-time*，配置路由器接口老化时间。
4. （可选）执行命令 **undo igmp-snooping router-learning** 禁止使能动态路由器接口学习功能。

   缺省情况下，使能动态路由器接口学习功能。禁止 VLAN 的路由器接口动态学习功能，VLAN 不再监听 IGMP Query 报文，只能手工配置静态路由器接口。

- 配置静态路由器接口
  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。

     这里的接口可以二层 GE 接口、二层 Ethernet 接口、二层 Eth-Trunk 接口。该接口是 AR2200-S 与上层路由器相连接的接口。
  3. 执行命令 **igmp-snooping static-router-port vlan** { { *vlan-id* [**to** *vlan-id*] } &<1-10> }，配置接口为静态路由器接口。

----结束

2.3.4 （可选）配置成员接口功能

背景信息

成员接口用来接收发往某组播组或组播源组的组播数据，缺省情况下为动态成员接口。当动态成员接口在其老化时间超时前没有收到该组播组的 IGMP 成员关系报告报文，设备将把该接口从该组播组所对应转发表项的出接口列表中删除。

当某个 VLAN 内的每个接口下都只有一个接收者主机时，可以使能该 VLAN 的接口快速离开功能。接口快速离开是指当设备从成员接口收到 IGMP Leave 消息时，不再等待转发表项老化，而是立即将该接口对应的转发表项从组播转发表中删除。

如果接口所连接的主机需要固定接收发往某组播组或组播源组的组播数据，可以配置该接口静态加入该组播组或组播源组，成为静态成员接口，静态成员接口不会老化。

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 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 配置成员接口老化时间。请参见 **2.3.5 （可选）配置 IGMP Snooping 查询器**。

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

步骤 4 （可选）执行命令 **igmp-snooping prompt-leave** [**group-policy** *acl-number*]，配置成员接口快速离开。

缺省情况下，不允许成员接口快速离开。

如果不指定 **group-policy** *acl-number* 参数，则 AR2200-S 只要从该 VLAN 内的成员接口收到离开消息，就对该接口做快速离开处理。

说明

在 AR2200-S 的实现中，默认 ACL 规则 **permit** 对所有组播组都适用，如果要配置针对某个组的快速离开功能，需要结合 **rule deny source any** 命令一起使用。

步骤 5 执行命令 **quit**，返回系统视图。

步骤 6 （可选）配置静态成员接口

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

   这里的接口可以是二层 GE 接口、二层 Ethernet 接口、二层 Eth-Trunk 接口。

2. （可选）执行命令 **undo igmp-snooping learning vlan** { *vlan-id* { [*&<1-10>*][**to** *vlan-id*] } }， 禁止组播成员接口动态学习功能。

   缺省情况下，使能接口的转发表项动态学习功能。禁止组播成员接口动态学习功能之后，如果要完成组播数据的转发，接口只能静态加入组播组。

3. 配置接口加入组播组

   - 执行命令 **l2-multicast static-group** [**source-address** *source-ip-address*] **group-address** *group-ip-address* **vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }，配置接口静态加入组播组，接口成为静态成员接口。
   - 执行命令 **l2-multicast static-group** [**source-address** *source-ip-address*] **group-address** *group-ip-address1* **to** *group-ip-address2* **vlan** *vlan-id* 批量将接口加入组播组。

----结束

2.3.5 （可选）配置 IGMP Snooping 查询器

背景信息

当上层路由器的 IGMP 报文因为某些原因不能到达 AR2200-S（例如未运行 IGMP 协议），或上层路由器的组播转发表项不需要动态学习而是静态配置时，可在本 AR2200-S 上配置查询器，代替上层路由器发送 IGMP Query 消息，同时根据网络需要，可以调整查询器的参数。

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 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping querier enable**，使能查询器功能。

缺省情况下，查询器功能处于禁止状态。

步骤 4 （可选）执行命令 **igmp-snooping query-interval** *query-interval*，配置查询器发送通用查询报文的时间间隔。

缺省情况下，通用查询时间间隔为 60 秒。

步骤 5 （可选）执行命令 **igmp-snooping robust-count** *robust-count*，配置查询器的 IGMP 健壮系数。

缺省情况下，IGMP 健壮系数为 2。

步骤 6 （可选）执行命令 **igmp-snooping max-response-time** *max-response-time*，配置查询器最大响应时间。

缺省情况下，IGMP 查询报文的最大响应时间是 10 秒。

说明

最大响应时间应小于通用查询时间间隔。

当 AR2200-S 收到主机的 IGMP Report 报文后，成员接口老化时间设置为：IGMP 健壮系数 × 通用查询时间间隔 + 最大响应时间。当参数都取缺省值时，成员接口老化时间缺省值为 130 秒。

步骤 7 （可选）执行命令 **igmp-snooping lastmember-queryinterval** *lastmember-queryinterval*，配置查询器发送特定组查询报文时间间隔。

缺省情况下，特定组查询时间间隔为 1 秒。

说明

当 AR2200-S 收到主机的 IGMP Leave 报文后，重置成员接口老化时间设置为：最后成员查询时间间隔（即特定组查询消息发送时间间隔） × IGMP 健壮系数。

由于运行 IGMPv1 时，主机离开组播组时不发送 IGMP Leave 报文，因此只有当 VLAN 内可以处理 IGMPv2 或者 IGMPv3 报文时，本配置才有意义。

----结束

2.3.6 （可选）配置接口加入最大组播组数量

背景信息

如果限制用户点播组播节目的数量，可配置接口加入的组播组最大数量，控制接口上的数据流量。

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。

这里的接口可以是二层 GE 接口、二层 Ethernet 接口、二层 Eth-Trunk 接口。

步骤 3 执行命令 **igmp-snooping group-limit** *group-limit* **vlan** { {*vlan-id* [**to** *vlan-id*] } &<1-10> }，配置接口加入的组播组最大数量。

缺省情况下，接口加入组播组的数量限制为 2000。

----结束

2.3.7 （可选）配置组播组策略

背景信息

在使能了 IGMP Snooping 的设备上，如果用户只想加入某些特定组播组或者限制用户加入任何组播组，通过配置组播组过滤器，可以限制用户对组播节目的点播。

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 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping group-policy** *acl-number* [**version** *number*]，配置组播组策略，使 VLAN 内的接口只能动态加入符合 ACL 规则的组播组。

缺省情况下，VLAN 没有配置组播组策略，即 VLAN 内的主机可以加入任何组播组。如果不指定应用组播组策略的 IGMP 报文版本，则 AR2200-S 对接收到的所有 IGMP 报文都应用该组播组策略。

说明

创建 VLAN 的组播组策略的 ACL 时，**rule** 命令必须使用参数 **deny** 才能生效，即只能通过配置 VLAN 的组播组策略禁止 VLAN 内的主机访问全部或指定组播组。

当配置的 group-policy 为高级 ACL 规则时，无论 ACL 规则配置什么协议字段，该 ACL 都默认会对组播组生效。

----结束

2.3.8 （可选）配置 IGMP 报文抑制功能

背景信息

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

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

在报文抑制时间内，AR2200-S 对用户发送的连续相同的 IGMP 报文只向上层设备转发一份，减少冗余报文。

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 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping report-suppress**，配置 VLAN 内对 Report 和 Leave 报文的抑制功能。

在配置了此命令后，AR2200-S 只会在组播组的第一个成员加入和最后一个成员离开时，向上游设备发送一条 Report 和 Leave 报文。

步骤 4 （可选）执行命令 **igmp-snooping suppress-time** *suppress-time*，配置当前 VLAN 内的 IGMP 报文抑制时间。

缺省情况下，IGMP 报文抑制时间为 10 秒。对 IGMP Report、IGMP Leave 报文的抑制时间最好等于当前 VLAN 的最大响应时间。

----结束

2.3.9 （可选）配置丢弃未知组播数据报文

背景信息

如果收到未知组播数据报文，缺省情况下在 VLAN 内广播。如果组播业务比较稳定，比如说静态二层组播业务，对于未知组播报文可以无需处理，可以配置丢弃未知组播数据报文。如果组播业务不太稳定，有组播用户频繁加入和退出的情况，对于未知组播报文必须进行处理，否则可能会导致部分用户无法接收到组播数据，必须配置丢弃未知组播数据报文。

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 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **multicast drop-unknown**，配置丢弃未知组播数据报文。

缺省情况下，VLAN 内的未知组播流的转发方式为在 VLAN 内广播。

----结束

2.3.10 （可选）配置 AR2200-S 主动发送 IGMP Query 报文

背景信息

当二层网络拓扑发生变化时，VLAN 报文的转发路径可能发生变化，配置主动发送 IGMP Query 报文，使 AR2200-S 感知二层网络拓扑变化，当组成员主机回应 IGMP Report 报文，AR2200-S 根据 IGMP Report 更新组成员接口信息，将组播数据流迅速切换到新的转发路径上，按照新的网络拓扑正确转发组播数据，从而保证业务不间断。

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 **igmp-snooping send-query enable**，配置 AR2200-S 的 IGMP Snooping 功能响应二层网络拓扑变化事件。缺省情况，禁止主动向非路由器接口发送 IGMP Query 报文。

说明

响应二层网络拓扑变化事件功能一般结合环网使用，当环网的拓扑发生变化时，AR2200-S 发送源 IP 地址为 192.168.0.1 的 IGMP 查询报文。该源地址可以通过 **igmp-snooping send-query source-address** *source-address* 命令进行修改。

----结束

2.3.11 （可选）配置对 IGMP 报文中 Router-Alert 选项的处理方式

背景信息

Router Alert 是一种标示协议报文的特殊机制，如果一个报文中带有 Router Alert 选项，则表示该报文需要被上送到路由协议层去处理。

缺省情况下设备不对 Router-Alert 选项进行检查，IGMP 报文中无论是否携带有 Router-Alert 选项，设备都会将其送给上层协议进行处理。为了提高设备性能、减少不必要的开支，同时出于协议安全性的考虑，可以配置设备接收或发送未携带 Router-Alert 选项的 IGMP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 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping require-router-alert**，配置接收的 IGMP 报文的 IP 头中必须带有 Router Alert。如果 AR2200-S 从当前 VLAN 内接收的 IGMP 报文的 IP 头中不带有 Router Alert，则 AR2200-S 不对报文进行处理，直接丢弃。

缺省情况下，AR2200-S 从 VLAN 内接收的 IGMP 报文的 IP 头中可以不带有 Router Alert。

步骤 4 执行命令 **igmp-snooping send-router-alert**，配置在 AR2200-S 发送的 IGMP 报文的 IP 头中携带 Router Alert 选项。使用 **undo igmp-snooping send-router-alert** 命令可以禁止在发送的 IGMP 报文的 IP 头中携带 Router Alert。

缺省情况下，AR2200-S 向 VLAN 内发送的 IGMP 报文的 IP 报文头中带有 Router Alert。

----结束

2.3.12 检查配置结果

前提条件

已完成 IGMP Snooping 配置。

操作步骤

- 使用命令 **display igmp-snooping configuration** 查看 IGMP Snooping 的配置信息。
- 使用命令 **display igmp-snooping** [**vlan** *vlan-id*]查看 VLAN 的 IGMP Snooping 配置信息。
- 使用命令 **display igmp-snooping statistics vlan** [*vlan-id*]查看 VLAN 的 IGMP Snooping 统计信息。
- 使用命令 **display igmp-snooping port-info** [**vlan** *vlan-id* [**group-address** *group-address*]] [**verbose**]查看组播组的成员接口信息。
- 使用命令 **display igmp-snooping router-port vlan** *vlan-id* 查看路由器接口信息。
- 使用命令 **display igmp-snooping querier vlan** [*vlan-id*]查看 IGMP Snooping 查询器使能信息。
- 使用命令 **display l2-multicast forwarding-table vlan** *vlan-id* [**source-address** *source-address*] **group-address** { *group-address* | **router-group** }查看 VLAN 的组播转发表信息。

----结束

任务示例

说明

没有使能 VLAN 下的 IGMP Snooping 功能时，各项配置也可以进行，但是不能生效。执行 **display igmp-snooping** [**vlan** *vlan-id*]命令也无效，即没有显示任何配置信息。

在配置成功时，执行 **display igmp-snooping** [**vlan** *vlan-id*]命令，应得到以下结果：

- VLAN 的 IGMP Snooping 功能应处于使能状态。
- 可以处理的 IGMP 报文的版本配置正确。
- VLAN 内的接口快速离开应配置正确。
- 路由器接口老化时间、最后成员查询时间间隔、通用查询时间间隔、最大响应时间和 IGMP 健壮系数配置正确。
- 组播组策略配置正确。
- Router Alert 配置正确。

例如：

```
<Huawei> display igmp-snooping vlan 3
  IGMP Snooping Information for VLAN 3
    IGMP Snooping is Enabled
    IGMP Version is 3
    IGMP Query Interval is Set to default 60
    IGMP Max Response Interval is Set to default 10
    IGMP Robustness is Set to default 2
    IGMP Last Member Query Interval is Set to default 1
    IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
    IGMP Filter Group-Policy 2000
    IGMP Prompt Leave Enable
    IGMP Require Router Alert
    IGMP Send Router Alert Enable
    IGMP Report Suppress Disable
    IGMP Suppress Time is set to default 10 seconds
    IGMP Querier Disable
    IGMP Router Port Learning Enable
    IGMP SSM-Mapping Disable
```

执行 **display igmp-snooping configuration** 命令，显示非缺省的配置信息。

例如：

```
<Huawei> display igmp-snooping configuration
 IGMP Snooping Configuration for VLAN 3
     igmp-snooping enable
     igmp-snooping version 3
     igmp-snooping require-router-alert
     igmp-snooping prompt-leave
     igmp-snooping group-policy 2000
```

执行 **display igmp-snooping statistics vlan** [*vlan-id*]命令，查看 IGMP Snooping 的统计信息。

例如：

```
<Huawei> display igmp-snooping statistics vlan 3
  IGMP Snooping Packets Counter
    Statistics for Vlan 3
    Recv V1 Report  16
    Recv V2 Report  8768
    Recv V3 Report  0
    Recv V1 Query   0
    Recv V2 Query   2243
    Recv V3 Query   0
    Recv Leave      215
    Recv Pim Hello  0
    Send Query(S=0) 0
    Send Query(S!=0)529
```

在禁止接口动态学习功能配置成功时，执行 **display igmp-snooping port-info** [**vlan** *vlan-id*] [**group-address** *group-address*] [**verbose**]命令，结果显示仅有静态表项；执行 **display igmp-snooping router-port vlan** *vlan-id* 命令，结果显示仅有静态路由器接口。例如：

```
<Huawei> display igmp-snooping port-info vlan 7
----------------------------------------------------------------------
                  (Source, Group)    Port                          Flag
----------------------------------------------------------------------
VLAN 7, 3 Entry(s)
                    (*, 225.1.1.1)    Eth2/0/3                      S--
                                                  1 port(s)
                    (*, 225.1.1.2)    Eth2/0/4                      S--
                                                  1 port(s)
                    (*, 225.1.1.3)    Eth2/0/5                      S--
                                                  1 port(s)
<Huawei> display igmp-snooping router-port vlan 3
Port Name                 UpTime   Expires     Flags
----------------------------------------------------------------
VLAN 3, 2 router-port(s)
Eth2/0/1                  1d:22h   00:01:20    DYNAMIC
Eth2/0/2                  2d:10h   --          STATIC
```

在使能查询器使能配置成功时，执行命令 **display igmp-snooping querier vlan** [*vlan-id*]，显示查询器使能正确。

```
<Huawei> display igmp-snooping querier vlan
VLAN                           Querier-state
-----------------------------------------------
3                              Enable
```

执行命令 **display l2-multicast forwarding-table vlan** 7，查看 VLAN7 的组播转发表信息。

```
<Huawei> display l2-multicast forwarding-table vlan 7
VLAN ID : 7, Forwarding Mode : IP
----------------------------------------------------------------------
                     (Source, Group)    Interface             Out-Vlan
----------------------------------------------------------------------
                        Router-port     Ethernet2/0/1            7
                      (*, 225.1.1.1)    Ethernet2/0/1            7
                                        Ethernet2/0/2            7
----------------------------------------------------------------------
Total Group(s) : 1
```

2.4 配置 IGMP Snooping 的 SSM Mapping 功能

介绍 IGMP Snooping 的 SSM Mapping 功能的配置方法。

2.4.1 建立配置任务

应用环境

SSM 相比传统 ISM 组播技术，可节省组播地址并有更好的安全性，但只有 IGMPv3 支持 SSM。目前大部分路由器支持 IGMPv3，但主机侧绝大部分仅支持 IGMPv1 或 IGMPv2，SSM Mapping 机制可以兼容运行 IGMPv3 之前版本的主机，使其也能够使用组播 SSM 范围的服务。

当上游设备最后一跳路由器运行 IGMPv3，并已部署 IGMP SSM Mapping，需要在与用户主机相连的二层设备 AR2200-S 上配置 IGMP Snooping SSM Mapping，与上层设备 IGMP SSM Mapping 对应一致。使组播组与组播源之间能够建立一一对应的映射关系，

将 IGMPv1 或 IGMPv2 数据报文中所包含的（*,G）信息映射为(S,G)信息，为用户主机提供 SSM 组播服务。

当用户主机加入组播组地址属于 ASM 类型，需要先在 AR2200-S 配置 SSM 组策略，将组播组地址加入到 SSM 组地址范围，再配置 IGMP Snooping 的 SSM Mapping 功能。

前置任务

在配置 IGMP Snooping 的 SSM Mapping 功能之前，需完成以下任务：

完成 IGMP Snooping 基本配置。

数据准备

在配置 IGMP Snooping 的 SSM Mapping 功能之前，需准备以下数据。

序号	数据
1	（可选）用于 SSM 组播策略的 ACL 规则
2	（可选）配置的 SSM 组策略
3	建立映射组播地址

2.4.2 （可选）配置 SSM 组策略

背景信息

如果用户加入的组播组地址为 ASM 型，需要先在 VLAN 上配置 SSM 组策略，将组播组地址加入到 SSM 组地址范围。

说明

创建 SSM 策略的 ACL 时，**rule** 命令必须使用参数 **permit** 并指定组播地址才能生效。如果配置参数 **deny** 或指定的地址不是组播地址，配置不生效。

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 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping ssm-policy** *basic-acl-number*,配置 SSM 组策略。

缺省情况下，SSM 组范围是 232.0.0.0 ～ 232.255.255.255。执行本命令配置 SSM 策略后，该策略允许的组都将作为 SSM 范围内的组对待。

----结束

2.4.3 配置 IGMP Snooping SSM Mapping

背景信息

配置 SSM Mapping 功能，使组播组与组播源之间能够建立一一对应的映射关系。

使能全局及 VLAN 的 IGMP Snooping 功能，VLAN 内 IGMP Snooping 的版本为 3，用户主机所属版本为 IGMPv1 或者 IGMPv2，需要配置 SSM Mapping 功能，此配置与上层设备的 IGMP SSM Mapping 对应一致。

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 **vlan** *vlan-id*，进入 VLAN 视图。

步骤 3 执行命令 **igmp-snooping version 3**，配置 VLAN 内 IGMP Snooping 的版本号为 3。

默认版本号为 2，但是 IGMPv2 版本不支持 SSM Mapping 功能。

步骤 4 执行命令 **igmp-snooping ssm-mapping enable**，使能 VLAN 内的 SSM Mapping 功能。

缺省情况下，组播 SSM Mapping 功能未使能。

步骤 5 执行命令 **igmp-snooping ssm-mapping** *ip-group-address* { *ip-group-mask* | *mask-length* } *ip-source-address*，配置指定范围内组播组地址与源地址映射。

指定范围的组播组地址为 SSM Policy 范围内的组播组地址。SSM Policy 配置方法请参见**（可选）配置 SSM 组策略**。

----结束

2.4.4 检查配置结果

前提条件

已完成 IGMP Snooping 的 SSM Mapping 功能的全部配置。

操作步骤

- 使用 **display igmp-snooping port-info** 命令查看端口表项信息。

----结束

任务示例

执行命令 **display igmp-snooping port-info**，可以查看对应的端口表项信息。例如：

```
<Huawei> display igmp-snooping port-info
 ----------------------------------------------------------------------
                    (Source, Group)  Port                          Flag
 ----------------------------------------------------------------------
 VLAN 10, 3 Entry(s)
              (10.1.1.2, 224.1.1.1)  Eth2/0/1                       --M
                                                1 port(s)
              (10.1.1.3, 224.1.1.1)  Eth2/0/1                       --M
                                                1 port(s)
              (10.1.1.4, 224.1.1.1)  Eth2/0/1                       --M
                                                1 port(s)
 ----------------------------------------------------------------------
```

2.5 维护

清除 IGMP Snooping 的统计数据。

2.5.1 清除组播转发表中的静态表项

背景信息

注意

静态表项被清除后无法自动恢复，直到再次被配置。确认需要清除组播转发表中的静态表项后，再执行以下命令。

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。

这里的接口可以是二层 GE 接口、二层 Ethernet 接口、二层 Eth-Trunk 接口。

步骤 3 执行命令 **undo l2-multicast static-group** [**source-address** *source-ip-address*] **group-address** *group-ip-address* **vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } & <1-10> }取消接口静态加入组播组的配置。也可以通过命令 **undo l2-multicast static-group** [**source-address** *source-ip-address*] **group-address** *group-ip-address1* **to** *group-ip-address2* **vlan** *vlan-id* 批量取消接口上加入的组播组地址。

----结束

2.5.2 清除组播转发表项

背景信息

注意

执行本命令会引起该 VLAN 内的主机接收某些组播流暂时性中断，直到主机再次发出 IGMP 成员报告消息，AR2200-S 重新生成转发表项后，主机才能再收到组播流。

操作步骤

- 在用户视图下使用命令 **reset igmp-snooping group** { **all** | **vlan** { *vlan-id* | **all** } }清除组播转发表中的动态转发表项。

说明

执行本命令不清除静态转发表项和动态路由器接口表项。

----结束

2.5.3 清除 IGMP Snooping 统计信息

背景信息

注意

清除 IGMP Snooping 的统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

- 在用户视图下使用命令 **reset igmp-snooping statistics** { **all** | **vlan** { *vlan-id* | **all** } }清除 IGMP Snooping 统计信息。

----结束

2.6 配置举例

介绍 IGMP Snooping 的配置举例。

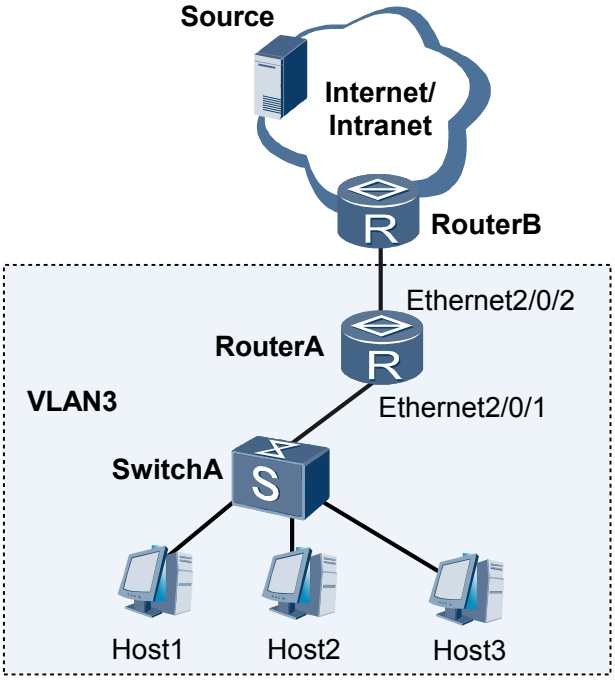
2.6.1 配置基于 VLAN 的 IGMP Snooping 示例

组网需求

如图 2-2 所示，RouterA 为 AR2200-S 设备，RouterA 的 Ethernet2/0/2 接口为静态路由器接口，连接组播源侧 RouterB，用来长期稳定接收组播数据。RouterA 的成员接口 Ethernet2/0/1 连接与用户直连的交换机。Ethernet2/0/2 和 Ethernet2/0/1 都加入同一 VLAN3。

在 VLAN 内 RouterA 上配置 IGMP Snooping，接口 Ethernet2/0/1 静态加入组播组地址 225.1.1.1 ～ 225.1.1.3，实现付费用户 Host1、Host2 和 Host3 在网络中通过组播方式能够长期稳定接收节目视频信息。

图 2-2 配置基于 VLAN 的 IGMP Snooping 组网图



配置思路

采用如下的思路配置 VLAN 中 IGMP Snooping 的功能：

1. 配置静态路由器接口，实现稳定接收组播数据。
2. 配置静态组播组地址 225.1.1.1 ～ 225.1.1.3，实现用户主机加入多个组播组，长期稳定接收组播数据。

数据准备

为完成此配置举例，需要准备以下数据：

- RouterA 的 Ethernet2/0/1 接口、Ethernet2/0/2 接口加入的 VLAN 编号 3。
- 静态路由器接口为 EthernetEthernet2/0/2。
- 静态组播组地址为 225.1.1.1 ～ 225.1.1.3。

操作步骤

步骤 1 创建 VLAN，配置接口加入 VLAN。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan 3
[RouterA-vlan3] quit
[RouterA] interface ethernet 2/0/2
[RouterA-Ethernet2/0/2] port hybrid pvid vlan 3
[RouterA-Ethernet2/0/2] port hybrid tagged vlan 3
[RouterA-Ethernet2/0/2] quit
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] port hybrid pvid vlan 3
```

```
[RouterA-Ethernet2/0/1] port hybrid untagged vlan 3
[RouterA-Ethernet2/0/1] quit
```

步骤 2 使能 IGMP Snooping 功能。

使能全局的 IGMP Snooping 功能。

```
[RouterA] igmp-snooping enable
```

使能 VLAN3 的 IGMP Snooping 功能。

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

步骤 3 配置 Ethernet2/0/2 为 VLAN3 的静态路由器接口。

```
[RouterA] interface ethernet 2/0/2
[RouterA-Ethernet2/0/2] igmp-snooping static-router-port vlan 3
[RouterA-Ethernet2/0/2] quit
```

步骤 4 配置静态组播组。

```
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] l2-multicast static-group group-address 225.1.1.1 vlan 3
[RouterA-Ethernet2/0/1] l2-multicast static-group group-address 225.1.1.2 vlan 3
[RouterA-Ethernet2/0/1] l2-multicast static-group group-address 225.1.1.3 vlan 3
[RouterA-Ethernet2/0/1] quit
[RouterA] quit
```

步骤 5 验证配置结果。

查看 VLAN 的 IGMP Snooping 配置信息。

```
<RouterA> display igmp-snooping vlan configuration
IGMP Snooping Configuration for VLAN 3
     igmp-snooping enable
```

由显示信息可知，VLAN 的 IGMP Snooping 功能已使能。

验证静态路由器接口配置。

在 RouterA 上执行命令 **display igmp-snooping router-port vlan 3**。

```
<RouterA> display igmp-snooping router-port vlan 3
 Port Name                UpTime    Expires   Flags
 ----------------------------------------------------------------------
 VLAN 3, 1 router-port(s)
 Eth2/0/2                 2d:10h    00:01:02  STATIC
```

由显示信息可知，Ethernet2/0/2 已被配置为静态路由器接口。

验证静态组播组的成员接口信息。

```
<RouterA> display igmp-snooping port-info
VLAN 3, 3 Entry(s)
----------------------------------------------------------------------
                  (Source, Group)    Port                          Flag
----------------------------------------------------------------------
                   (*, 225.1.1.1)    Ethernet2/0/1                 S--
                                          1 port(s)
                   (*, 225.1.1.2)    Ethernet2/0/1                 S--
                                          1 port(s)
                   (*, 225.1.1.3)    Ethernet2/0/1                 S--
                                          1 port(s)
```

由显示信息可知，225.1.1.1 ～ 225.1.1.3 已被配置为静态表项。

查看组播转发表项。

```
<RouterA> display l2-multicast forwarding-table vlan 3
VLAN ID : 3, Forwarding Mode : IP
------------------------------------------------------------------------------
                     (Source, Group)     Interface              Out-Vlan
------------------------------------------------------------------------------
                        Router-port      Ethernet2/0/2            3
                    (*, 225.1.1.1)       Ethernet2/0/1            3
                                         Ethernet2/0/2            3
                    (*, 225.1.1.2)       Ethernet2/0/1            3
                                         Ethernet2/0/2            3
                    (*, 225.1.1.3)       Ethernet2/0/1            3
                                         Ethernet2/0/2            3
------------------------------------------------------------------------------
Total Group(s) : 3
```

由显示信息可知 225.1.1.1 ～ 225.1.1.3 的数据在转发表中对应的 VLAN 和接口。

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 vlan batch 3
#
 igmp-snooping enable
#
vlan 3
 igmp-snooping enable
#
interface Ethernet2/0/1
 port hybrid pvid vlan 3
 port hybrid untagged vlan 3
 l2-multicast static-group group-address 225.1.1.1 to 225.1.1.3 vlan 3
#
interface Ethernet2/0/2
 port hybrid pvid vlan 3
 port hybrid tagged vlan 3
 igmp-snooping static-router-port vlan 3
#
return
```

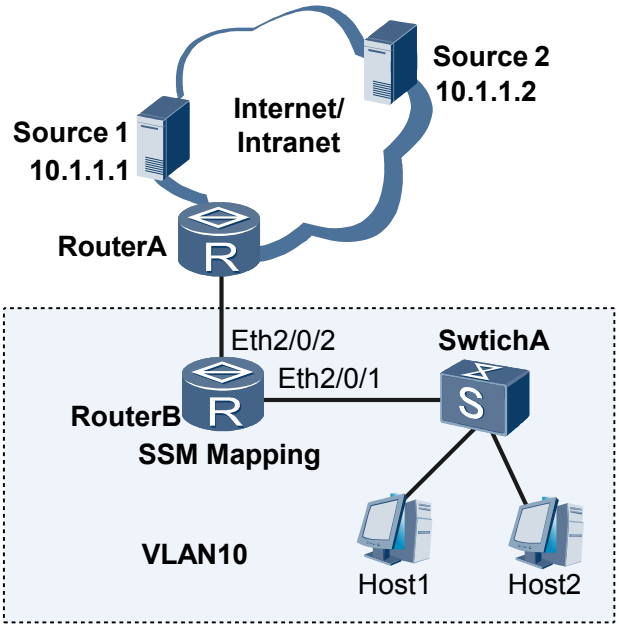
2.6.2 配置 IGMP Snooping 的 SSM Mapping 功能示例

组网需求

如图 2-3 所示的组网中，SwitchA 和用户主机 Host1 和 Host2 运行的软件版本都为 IGMPv2，组播源侧最后一跳路由器 RouterA 运行 IGMPv3。RouterB 为 AR2200-S 作为二层设备，RouterB 的 Ethernet2/0/2 接口连接 RouterA，Ethernet2/0/1 接口与 SwitchA 相连，加入 VLAN10。RouterB 的 Ethernet2/0/2 接口为静态路由器接口，成员接口 Ethernet2/0/1 静态加入组播组地址 224.1.1.1。Ethernet2/0/1 和 Ethernet2/0/2 都加入同一 VLAN10，并且上层设备 RouterA 已部署 IGMP SSM Mapping 功能。

在 VLAN 内 RouterB 上配置 IGMP Snooping 的 SSM Mapping 功能，与三层 IGMP SSM Mapping 对应一致，使组播组与组播源之间能够建立一一对应的映射关系，将 IGMPv1 或 IGMPv2 数据报文中所包含的（*,G）信息映射为(S,G)信息，实现用户 Host1 和 Host2 不升级主机，在当前运行的 IGMPv2 版本上指定组播源，点播相应的节目，为其提供 SSM 组播服务。

图 2-3 配置组播 SSM Mapping 功能组网图



配置思路

采用如下的思路配置 IGMP Snooping 的 SSM Mapping 功能：

1. 配置 IGMP Snooping 的基本功能，实现用户接收组播源数据。
2. 配置 IGMP Snooping 的 SSM 组策略，实现用户所在的 ASM 类型组播组地址加入到 SSM 组地址范围内。
3. 配置 IGMP Snooping 的 SSM Mapping 功能，实现用户接收指定组播源数据。

数据准备

为完成此配置例，需准备如下的数据：

- RouterB 的 Ethernet2/0/1 接口、Ethernet2/0/2 接口加入的 VLAN 编号 10。
- RouterB 运行版本为 IGMPv3，SwitchA、Host1 和 Host2 运行版本为 IGMPv2。
- 指定组播源地址 10.1.1.2。
- 静态组播组地址为 224.1.1.1。

操作步骤

步骤 1 配置 VLAN

配置 RouterB。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] vlan 10
[RouterB-vlan10] quit
[RouterB] interface ethernet 2/0/2
[RouterB-Ethernet2/0/2] port hybrid pvid vlan 10
[RouterB-Ethernet2/0/2] port hybrid tagged vlan 10
```

```
[RouterB-Ethernet2/0/2] quit
[RouterB] interface ethernet 2/0/1
[RouterB-Ethernet2/0/1] port hybrid pvid vlan 10
[RouterB-Ethernet2/0/1] port hybrid untagged vlan 10
[RouterB-Ethernet2/0/1] quit
```

步骤 2 使能全局和 VLAN 下 IGMP Snooping 功能

配置 RouterB。

```
[RouterB] igmp-snooping enable
[RouterB] vlan 10
[RouterB-vlan10] igmp-snooping enable
```

步骤 3 RouterB 运行 IGMP 版本号为 IGMPv3，用户主机运行 IGMP 版本号为 IGMPv2，且不允许将用户主机升级到 IGMPv3

配置 RouterB。

```
[RouterB-vlan10] igmp-snooping version 3
[RouterB-vlan10] quit
```

步骤 4 VLAN10 内配置 Ethernet2/0/2 接口为静态路由器接口，Ethernet2/0/1 接口静态加入组播组地址为 224.1.1.1 的组播组

```
[RouterB] interface ethernet 2/0/2
[RouterB-Ethernet2/0/2] igmp-snooping static-router-port vlan 10
[RouterB-Ethernet2/0/2] quit
[RouterB] interface ethernet 2/0/1
[RouterB-Ethernet2/0/1] l2-multicast static-group  group-address 224.1.1.1 vlan 10
[RouterB-Ethernet2/0/1] quit
```

步骤 5 配置 IGMP Snooping 的 SSM 组策略和 SSM Mapping 功能

```
[RouterB] acl number 2008
[RouterB-acl-basic-2008] rule 5 permit source 224.1.1.1 0
[RouterB-acl-basic-2008] quit
[RouterB] vlan 10
[RouterB-vlan10] igmp-snooping ssm-policy 2008
[RouterB-vlan10] igmp-snooping ssm-mapping enable
[RouterB-vlan10] igmp-snooping ssm-mapping 224.1.1.1 24 10.1.1.2
[RouterB-vlan10] quit
```

步骤 6 检查配置结果

在 RouterB 上执行 **display igmp-snooping vlan configuration** 命令，查看 VLAN 内配置情况。

```
[RouterB] display igmp-snooping vlan configuration
 IGMP Snooping Configuration for VLAN 10
     igmp-snooping enable
     igmp-snooping version 3
     igmp-snooping ssm-mapping enable
     igmp-snooping ssm-policy 2008
     igmp-snooping ssm-mapping 224.1.1.0 255.255.255.0 10.1.1.2
```

当 RouterB 收到组播 Report 报文时，执行 **display igmp-snooping port-info** 命令，查看端口信息。

```
[RouterB] display igmp-snooping port-info
 ----------------------------------------------------------------------
                  (Source, Group)  Port                          Flag
 ----------------------------------------------------------------------
 VLAN 10, 1 Entry(s)
              (10.1.1.2, 224.1.1.1)  Eth2/0/1                    --M
                                              1 port(s)
 ----------------------------------------------------------------------
```

----结束

配置文件

- RouterB 的配置文件

```
#
 sysname RouterB
#
 vlan batch 10
#
 igmp-snooping enable
#
vlan 10
 igmp-snooping enable
 igmp-snooping ssm-mapping enable
 igmp-snooping version 3
 igmp-snooping ssm-policy 2008
 igmp-snooping ssm-mapping 224.1.1.0 255.255.255.0 10.1.1.2
#
acl number 2008
 rule 5 permit source 224.1.1.1 0
#
interface Ethernet2/0/1
 port hybrid untagged vlan 10
 l2-multicast static-group  group-address 224.1.1.1 vlan 10
#
interface Ethernet2/0/2
 port hybrid pvid vlan 10
 port hybrid tagged vlan 10
 igmp-snooping static-router-port vlan 10
#
return
```

3 IGMP 配置

关于本章

在与用户网段相连的组播设备接口上配置 IGMP 协议，可以实现对本地网络组成员的管理。

3.1 IGMP 概述
IGMP 协议即因特网组管理协议，分为 IGMPv1、IGMPv2 和 IGMPv3 三个版本，均支持 ASM 模型，IGMPv3 可直接支持 SSM 模型。

3.2 AR2200-S 支持的 IGMP 特性
系统支持的 IGMP 特性包括：IGMP 基本功能、Router-Alert 选项、IGMP 查询控制器、SSM-Mapping、IGMP 组成员关系个数限制和 IGMP Report 报文主机地址过滤。

3.3 配置 IGMP 的基本功能
通过在与用户网段相连的组播设备接口上配置 IGMP 基本功能，用户主机可以接入组播网络，组播报文能够到达接收者。

3.4 配置 IGMP 报文选项
系统支持配置 IGMP 报文选项过滤 IGMP Report 报文，包括：配置拒绝接收无 Router-Alert 选项的 IGMP 报文、发送无 Router-Alert 选项的 IGMP 报文和 IGMP Report 报文主机地址过滤。

3.5 配置 IGMP 查询控制
IGMP 查询器周期性发送查询报文，刷新该网段的组成员信息。同一网段内所有与用户网段相连的组播设备接口配置的 IGMP 参数信息必须完全一致，否则将导致网络故障。

3.6 配置 SSM Mapping
在提供 SSM 模式服务的组播网络中，组播设备接口运行 IGMPv3，某些用户主机只能运行 IGMPv1/v2。为保证高版本组播设备兼容低版本主机并向这些用户提供 SSM 服务，在组播设备上配置 SSM Mapping 静态映射功能。

3.7 配置 IGMP Limit 功能
当运营商希望限制可服务的 IPTV ICP 及用户接入的数量时，可配置 IGMP Limit 功能。IGMP Limit 功能包括：全局 IGMP 组成员关系个数限制、单实例 IGMP 全局表项限制和基于接口的 IGMP 组成员关系个数限制。

3.8 维护 IGMP
IGMP 的维护包括：清除 IGMP 的组信息。

3.9 配置举例

针对如何在组播网络中配置 IGMP 基本功能、SSM-Mapping、以及 IGMP Limit，分别提供配置举例。

3.1 IGMP 概述

IGMP 协议即因特网组管理协议，分为 IGMPv1、IGMPv2 和 IGMPv3 三个版本，均支持 ASM 模型，IGMPv3 可直接支持 SSM 模型。

随着组播应用的发展，加入组播组接收组播数据的主机越来越多，如何在路由器上管理组播组和相应的成员成为一个重要问题。

IGMP（Internet Group Management Protocol）作为因特网组管理协议，是 TCP/IP 协议族中负责 IPv4 组播成员管理的协议，它用来在 IP 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。

IGMP 协议是 IP 组播在末端网络上使用的主机对路由器的信令机制，分为两个功能部分：主机侧和路由器侧。

说明

主机支持 IGMP 的具体情况和所使用的操作系统有关。

- 所有参与组播传输的接收者主机必须应用 IGMP 协议。主机可以在任意时间、任意位置、成员总数不受限制地加入或退出组播组。
- 支持组播的路由器通过 IGMP 协议了解每个接口连接的网段上是否存在某个组播组的接收者，即组成员。而各主机只需要保存自己加入了哪些组播组。

到目前为止，IGMP 有三个版本：IGMPv1 版本（由 RFC1112 定义）、IGMPv2 版本（由 RFC2236 定义）和 IGMPv3（由 RFC3376 定义）版本。所有 IGMP 版本都支持 ASM（Any-Source Multicast）模型。IGMPv3 可以直接应用于 SSM（Source-Specific Multicast）模型，而 IGMPv1 和 IGMPv2 则需要 SSM Mapping 技术的支持。

3.2 AR2200-S 支持的 IGMP 特性

系统支持的 IGMP 特性包括：IGMP 基本功能、Router-Alert 选项、IGMP 查询控制器、SSM-Mapping、IGMP 组成员关系个数限制和 IGMP Report 报文主机地址过滤。

说明

异步串口，ISDN BRI 接口，3G 接口，Bridge-if 接口，NULL 接口，QinQ 子接口不支持 IGMP。

IGMP 基本功能

AR2200-S 支持的 IGMP 基本功能有：

- 支持 IGMPv1、IGMPv2 和 IGMPv3，版本可配置。
- 支持静态 IGMP。
- 允许配置接口加入的组播组范围。

目前，AR2200-S 支持的 IGMPv3 可以处理以下报文：

- 组地址属于 SSM 范围。
- 组地址属于 ASM 范围，组记录类型是 MODE_IS_EXCLUDE 或 CHANGE_TO_EXCLUDE_MODE，且源地址列表为空。

其他类型的报文均不予处理。

Router-Alert 选项

IGMP 通过 Router-Alert 选项来将送往本地的没有加入的组报文送到上层协议进行处理。

用户可以根据需要配置是否在发送的 IGMP 报文中包含 Router-Alert 选项、是否要求接收的 IGMP 报文必须包含 Router-Alert 选项。

IGMP 查询控制器

对于 IGMPv1，用户可以设置普遍组查询消息的发送间隔、健壮系数。

对于 IGMPv2，用户可以配置普遍组查询消息的发送间隔、健壮系数、IGMP 查询报文的最大响应时间、IGMP 快速离开等功能。

对于 IGMPv3，用户可以配置普遍组查询消息的发送间隔、健壮系数、IGMP 查询报文的最大响应时间等功能。

SSM-Mapping

用户可以通过在路由器上配置 SSM-Mapping 功能，向运行 IGMPv1 或 IGMPv2 的主机提供服务。

限制 IGMP 组成员关系个数

- 限制全局 IGMP 组成员关系个数：路由器创建的所有 IGMP 组成员关系个数不能超过限制值，当达到限制值时不允许创建新的 IGMP 表项。
- 限制单实例下所有 IGMP 组成员关系个数：与实例相关的所有 IGMP 组成员关系个数不能超过限制值。当达到限制值时不允许创建新的 IGMP 表项。
- 限制接口下所有 IGMP 组成员关系个数：接口下创建的所有 IGMP 组成员关系个数不能超过限制值。当达到限制值时不允许创建新的 IGMP 表项。

IGMP Report 报文主机地址过滤

通过固定的主机地址过滤规则，可以实现对 IGMP Report 报文主机地址的过滤。

3.3 配置 IGMP 的基本功能

通过在与用户网段相连的组播设备接口上配置 IGMP 基本功能，用户主机可以接入组播网络，组播报文能够到达接收者。

3.3.1 建立配置任务

在配置 IGMP 的基本功能前了解此特性的应用环境、配置此特性的前置任务以及需要进行的数据准备，可以快速、准确地完成配置任务。

应用环境

IGMP 应用在路由器与用户相连的网段，在路由器和用户主机上都需要运行 IGMP。本节只介绍如何在路由器上配置 IGMP。

配置 IGMP 之前，必须先使能 IP 组播路由。IP 组播路由是配置一切组播功能的前提。如果停止 IP 组播路由，与组播相关的所有配置将被删除。

在连接用户主机的接口上使能 IGMP，由于不同版本的 IGMP 协议报文不相同，因此需要为路由器和主机配置匹配的版本（路由器侧的高版本可以兼容主机侧的低版本）。执行此操作之后，才能进行 IGMP 的其他配置。

为了让接口所连接网络上的主机加入指定的组播组，并接收这些组的报文，可以在对应接口上设置一个 ACL 过滤规则，以限制接口所服务的组播组范围。

前置任务

在配置 IGMP 的基本功能之前，需完成以下任务：

- 配置接口的链路层协议参数和 IP 地址，使接口的链路协议状态为 Up。
- 配置单播路由协议，使各节点间 IP 路由可达。

数据准备

在配置 IGMP 基本功能之前，需准备以下数据。

序号	数据
1	IGMP 版本
2	用于配置组播静态路由的组播组地址、组播源地址
3	（可选）过滤组播组地址的 ACL 规则

说明

- 在 IGMP 视图下的配置全局有效，在接口视图下的配置只对该接口有效。
- 如果接口视图和 IGMP 视图下都配置了命令，则优先选择接口视图下配置的值。

3.3.2 使能 IP 组播路由

使能组播路由是配置组播功能的首要步骤。

背景信息

请在与用户主机相连的路由器上进行以下配置。

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 **multicast routing-enable**，使能公网实例 IP 组播路由。

缺省情况下，路由器未使能公网实例 IPv4 组播路由。

----结束

3.3.3 使能 IGMP 功能

在与用户网段相连的组播设备接口上使能 IGMP，用户主机可以动态加入组播组。

背景信息

在与用户主机相连的路由器上进行如下配置。

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。

interface-type interface-number 是与用户主机相连的接口。

步骤 3 执行命令 **igmp enable**，使能 IGMP 功能。

缺省情况下，接口上未使能 IGMP 功能。

----结束

3.3.4 （可选）配置 IGMP 版本

在与用户网段相连的组播设备接口上配置 IGMP 版本。同一网段内所有与用户网段相连的组播设备配置的 IGMP 版本必须相同，否则将导致网络故障。

背景信息

请务必保证同一网段的所有 IGMP 路由器接口配置的 IGMP 版本都相同，缺省采用 IGMPv2 版本。

在与用户主机相连的路由器上进行如下配置。

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 **igmp version** { **1** | **2** | **3** }，配置接口的 IGMP 版本。

----结束

3.3.5 （可选）配置静态 IGMP 组

在与用户网段相连的组播设备接口配置静态加入 IGMP 组播组，组播设备认为该接口上始终连接着组成员，并持续向该接口转发符合条件的组播报文。

背景信息

在与用户主机相连的路由器上进行如下配置。

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 **igmp static-group** *group-address* [**inc-step-mask** { *group-mask* | *group-mask-length* } **number** *group-number*] [**source** *source-address*]，配置静态加入批量组播组或单个组播组。静态加入组播组后，认为路由器该接口所在网段上存在所配置静态组的成员。

----结束

3.3.6 （可选）配置允许接口加入的组播组范围

用户主机加入组播组时，可以在与用户网段相连的组播设备接口上配置此功能，限制用户主机能够加入的组播组范围。

背景信息

在与用户主机相连的路由器上进行如下配置。

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 **igmp group-policy** { *acl-number* | **acl-name** *acl-name* } [**1** | **2** | **3**]，配置允许接口加入的组播组范围。

缺省情况下，允许接口加入任何组播组。

----结束

3.3.7 检查配置结果

配置 IGMP 基本功能成功后，查看接口上的 IGMP 配置和运行信息、以及 IGMP 组播组的成员信息，确保 IGMP 正常运行。

操作步骤

- 使用 **display igmp interface** [*interface-type interface-number* | **up** | **down**] [**verbose**] 命令查看接口上的 IGMP 配置和运行信息。
- 使用 **display igmp group** [*group-address* | **interface** *interface-type interface-number*] * **static** 命令查看静态 IGMP 组播组的成员信息。
- 使用 **display igmp group** [*group-address* | **interface** *interface-type interface-number*] * **verbose** 命令查看 IGMP 组播组的成员信息。

----结束

3.4 配置 IGMP 报文选项

系统支持配置 IGMP 报文选项过滤 IGMP Report 报文，包括：配置拒绝接收无 Router-Alert 选项的 IGMP 报文、发送无 Router-Alert 选项的 IGMP 报文和 IGMP Report 报文主机地址过滤。

3.4.1 建立配置任务

在配置 IGMP 报文选项前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以快速、准确地完成配置任务。

应用环境

Router-Alert 选项用于将未指定接收组播组的 IGMP 报文送到上层协议进行处理。关于 Router-Alert 的相关介绍，请参考 RFC2113。

前置任务

在配置 IGMP 报文选项之前，需完成以下任务：

- 配置某单播路由协议，使整个组播域连通
- **配置 IGMP 的基本功能**

数据准备

在配置 IGMP 报文选项之前，需准备以下数据：

序号	数据
1	是否需要报文中包含 Router-Alert 选项
2	需要过滤 IGMP Report 报文的接口类型和编号

3.4.2 配置拒绝接收无 Router-Alert 选项的 IGMP 报文

与用户网段相连的组播设备只接收包含 Router-Alert 的 IGMP 报文，可在与用户网段相连的组播设备上配置拒绝接收无 Router-Alert 选项的 IGMP 报文。缺省情况下，组播设备处理接收到的所有 IGMP 报文。

背景信息

缺省情况下，路由器不对 IGMP 报文中携带 Router-Alert 选项进行检查，即处理所有接收到的 IGMP 报文，包括无 Router-Alert 选项的 IGMP 报文。

当用户不希望接收无 Router-Alert 选项的 IGMP 报文时，可在与用户相连的路由器上进行如下配置。

说明

此项配置可以在两种情况下进行:

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局取值，未配置接口值时，接口的取值和全局取值保持一致。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **igmp**，进入 IGMP 视图。
  3. 执行命令 **require-router-alert**，配置要求接收到的 IGMP 报文包含 Router-Alert 选项，如果未包含 Router-Alert 选项则丢弃。
- 接口
  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。

     该接口是与用户主机或交换设备相连的接口。
  3. 执行命令 **igmp require-router-alert**，配置要求接收到的 IGMP 报文包含 Router-Alert 选项，如果未包含 Router-Alert 选项则丢弃。

----结束

3.4.3 配置发送无 Router-Alert 选项的 IGMP 报文

同一网段的其他 IGMP 接口需要接收无 Router-Alert 的报文，可在与用户网段相连的组播设备上配置发送的 IGMP 报文中不包含 Router-Alert 选项。缺省情况下，组播设备发送的 IGMP 报文中携带 Router-Alert 选项。

背景信息

缺省情况下，路由器发送的 IGMP 报文中携带 Router-Alert 选项。

当需要发送无 Router-Alert 选项的 IGMP 报文时，可在与用户相连的路由器上进行如下配置。

说明

此项配置可以在两种情况下进行:

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局取值，未配置接口值时，接口的取值和全局取值保持一致。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **igmp**，进入 IGMP 视图。
  3. 执行命令 **undo send-router-alert**，配置在发送的 IGMP 报文头不包含 Router-Alert 选项。
- 接口
  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。

   该接口是与用户主机或交换设备相连的接口。

3. 执行命令 **undo igmp send-router-alert**，配置在发送的 IGMP 报文头中不包含 Router-Alert 选项。

----结束

3.4.4 配置 Report 报文主机地址过滤

IGMP Report 报文主机地址过滤是一种安全策略，可过滤掉非本网段用户发送的 IGMP Report 报文。配置此功能后，设备丢弃主机地址和接收报文的接口地址不在同一网段的 IGMP Report 报文。

背景信息

缺省情况下，路由器不对 IGMP Report 报文的主机地址进行过滤，即处理所有接收到的 IGMP Report 报文。

IGMP Report 报文主机地址的过滤规则是：

- 处理主机地址和接收报文的接口地址在同一网段，或者主机地址是 0.0.0.0 的 IGMP 报文。
- 丢弃主机地址和接收报文的接口地址不在同一网段的 IGMP 报文。

当用户希望过滤 IGMP Report 报文的主机地址时，可在路由器与用户相连的接口上进行如下配置。

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 **igmp ip-source-policy**，过滤 IGMP Report 报文的主机地址。

----结束

3.4.5 检查配置结果

配置 IGMP 报文选项成功后，查看 IGMP 组播组的成员信息、接口上的 IGMP 配置和运行信息，确保 IGMP 正常运行。

操作步骤

- 使用 **display igmp group** [*group-address* | **interface** *interface-type interface-number*] * [**static**] [**verbose**]命令查看 IGMP 组播组的成员信息。
- 使用 **display igmp interface** [*interface-type interface-number* | **up** | **down**] [**verbose**] 命令查看接口上 IGMP 配置和运行信息。

----结束

3.5 配置 IGMP 查询控制

IGMP 查询器周期性发送查询报文，刷新该网段的组成员信息。同一网段内所有与用户网段相连的组播设备接口配置的 IGMP 参数信息必须完全一致，否则将导致网络故障。

3.5.1 建立配置任务

在配置 IGMP 查询控制前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以快速、准确地完成配置任务。

应用环境

注意

IGMP 接口参数众多并且相互制约，请务必保证同一网段的所有 IGMP 路由器接口的所有 IGMP 参数配置信息完全一致，否则将导致网络故障。

在与接收者相连的共享网段上，由 IGMP 查询器周期性地发送查询报文，当得到某一组成员报告时，刷新该网段相应的组成员关系信息。

如果非查询器在“其他 IGMP 查询器存活时间”之内没有收到普遍查询报文，则认为查询器故障，将自动发起新一轮的查询器选举过程。

在 ADSL 拨号上网应用中，由于一台主机对应一个端口，因此查询器仅对应一个接收者主机，当接收者主机在多个组播组间频繁切换（例如电视选台），可以在查询器上启动立刻离开组机制。

前置任务

在配置 IGMP 查询控制之前，需完成以下任务：

- 配置某单播路由协议，使整个组播域连通
- **配置 IGMP 的基本功能**

数据准备

在配置 IGMP 查询控制之前，需准备以下数据。

序号	数据
1	IGMP 普遍组查询消息的发送间隔
2	健壮系数
3	IGMP 查询消息的最大响应时间
4	其他 IGMP 查询器存活时间
5	IGMP 最后成员查询消息的发送间隔

序号	数据
6	限定快速离开应用范围的 ACL

3.5.2 配置 IGMPv1 查询器

IGMPv1 查询器的功能包括：普遍组查询消息的发送间隔和健壮系数。

背景信息

在与用户主机相连的路由器上进行如下配置。此项配置可选。

说明

此项配置可以在两种情况下进行:

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

此配置做为成员动态老化时间的功能时，请在三层设备中与上游二层设备进行相同配置，否则会影响组播数据在二层网络与三层网络之间的正常传输。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **igmp**，进入 IGMP 视图。
  3. 执行命令 **timer query** *interval*，配置普遍组查询消息的发送间隔。

     缺省情况下，“普遍查询消息发送间隔”为 60 秒。
  4. 执行命令 **robust-count** *robust-value*，配置 IGMP 健壮系数。

     缺省情况下，IGMP 健壮系数为 2。
- 接口
  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 **igmp timer query** *interval*，配置普遍组查询消息的发送间隔。

     缺省情况下，“普遍查询消息发送间隔”为 60 秒。
  4. 执行命令 **igmp robust-count** *robust-value*，配置 IGMP 健壮系数。

     缺省情况下，IGMP 健壮系数为 2。

----结束

3.5.3 配置 IGMPv2/v3 的查询器

IGMPv2/v3 查询器的功能包括：普遍组查询消息的发送间隔、健壮系数、查询报文最大响应时间、其他查询器存活时间、最后成员查询报文发送间隔、指定组查询报文发送间隔、接口上组成员关系永不超时、以及 IGMP 快速离开。

背景信息

注意

在实际配置中，请确保：“最大响应时间”<“普遍查询消息发送间隔”<“其他 IGMP 查询器的存活时间”。

在与用户主机相连的路由器上进行如下配置。此项配置可选。

说明

此项配置可以在两种情况下进行：

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

此配置做为成员动态老化时间的功能时，请在三层设备与下游二层设备上进行相同配置，否则会影响组播数据在二层网络与三层网络之间的正常传输。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **igmp**，进入 IGMP 视图。
  3. 执行命令 **timer query** *interval*，配置普遍组查询消息的发送间隔。缺省情况下，“普遍查询消息发送间隔”为 60 秒。
  4. 执行命令 **robust-count** *robust-value*，配置 IGMP 健壮系数。缺省情况下，IGMP 健壮系数为 2。

     当路由器启动时发送“健壮系数”次的“普遍组查询消息”，发送间隔为“IGMP 普遍组查询消息的发送间隔”的 1/4。当路由器收到离开消息后，

     - 对于 IGMPv2，路由器发送“健壮系数”次的“特定组查询消息”，发送间隔为“IGMP 特定组查询消息的发送间隔”。
     - 对于 IGMPv3，路由器发送“健壮系数”次的“特定组/源查询消息”，发送间隔为“IGMP 特定组/源查询消息的发送间隔”。

     “健壮系数”越大，IGMP 路由器就越健壮，但是组超时的时间也就越长。
  5. 执行命令 **max-response-time** *interval*，配置 IGMP 查询报文的最大响应时间。缺省情况下，IGMP 最大响应时间为 10 秒。
  6. 执行命令 **timer other-querier-present** *interval*，配置其他 IGMP 查询器存活时间。缺省情况下，“其他 IGMP 查询器的存活时间”＝“健壮系数”×“普遍查询消息发送间隔”+（1/2）×“最大响应时间”。当“健壮系数”、“普遍查询消息发送间隔”和“最大响应时间”都取缺省值时，“其他 IGMP 查询器的存活时间”的值为 125 秒。
  7. 执行命令 **lastmember-queryinterval** *interval*，配置 IGMP 最后成员查询报文的发送间隔。发送间隔越小，查询器就越灵敏。缺省情况下，时间间隔为 1 秒。
- 接口
  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 **igmp timer query** *interval*，配置普遍组查询消息的发送间隔。缺省情况下，IGMP 普遍组查询消息的发送间隔是 60 秒。
4. 执行命令 **igmp max-response-time** *interval*，配置 IGMP 查询报文的最大响应时间。缺省情况下，IGMP 查询报文的最大响应时间是 10 秒。
5. 执行命令 **igmp timer other-querier-present** *interval*，配置其他 IGMP 查询器存活时间。缺省情况下，其他 IGMP 查询器的存活时间的计算公式是：其他 IGMP 查询器的存活时间 = 健壮系数 × IGMP 普遍查询消息发送间隔 +（1/2）× 最大查询响应时间。当健壮系数、IGMP 普遍查询消息发送间隔和最大查询响应时间都取缺省值时，其他 IGMP 查询器的存活时间的值为 125 秒。
6. 执行命令 **igmp robust-count** *robust-value*，配置 IGMP 健壮系数。缺省情况下，IGMP 查询器的健壮系数是 2。
7. 执行命令 **igmp lastmember-queryinterval** *interval*，配置 IGMP 指定组查询报文的发送间隔。缺省情况下，发送 IGMP 最后组成员查询报文的时间间隔是 1 秒。
8. 执行命令 **igmp on-demand**，配置接口上的组成员关系永不超时，接口不向外发送 IGMP 查询报文。缺省情况下，接口参与查询器选举，发送查询报文。

   说明

   此命令适用于 IGMPv2 和 IGMPv3。
9. 执行命令 **igmp prompt-leave** [**group-policy** { *basic-acl-number* | **acl-name** *acl-name* }]，配置 IGMP 快速离开。当接口接收到某组播组的离开消息时，不发送最后成员查询消息，立即删除接口上的组成员关系。

   缺省情况下，IGMP 将在接收到主机发送的离开消息后发送最后成员查询消息。

   说明

   本命令只对 IGMPv2 有效。

----结束

3.5.4 检查配置结果

配置 IGMP 查询控制成功后，查看接口上 IGMP 的配置和运行信息，以及 IGMP 路由表信息，确保 IGMP 正常运行。

操作步骤

- 使用 **display igmp interface** [*interface-type interface-number* | **up** | **down**] [**verbose**] 命令查看接口上 IGMP 配置和运行信息。
- 使用 **display igmp routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }]] * [**static**] [**outgoing-interface-number** [*number*]]命令查看 IGMP 路由表信息。

  说明

  在接口上只配置了 IGMP，没有配置 PIM，且接口为查询器的情况下，才会生成 IGMP 路由表项。可以使用 **display igmp routing-table** 命令查看 IGMP 路由表。

----结束

3.6 配置 SSM Mapping

在提供 SSM 模式服务的组播网络中，组播设备接口运行 IGMPv3，某些用户主机只能运行 IGMPv1/v2。为保证高版本组播设备兼容低版本主机并向这些用户提供 SSM 服务，在组播设备上配置 SSM Mapping静态映射功能。

3.6.1 建立配置任务

在配置 SSM Mapping 前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以快速、准确地完成配置任务。

应用环境

在提供 SSM 模式组播服务的网段中，由于各种可能的限制，某些用户主机必须运行 IGMPv1 或 v2。为保证向这些用户提供 SSM 服务，需要在路由器上配置 SSM 静态映射功能。

前置任务

在配置 SSM Mapping 之前，需完成以下任务：

- 配置某单播路由协议，使整个组播域连通
- **使能 IP 组播路由**

数据准备

在配置 SSM Mapping 之前，需准备以下数据。

序号	数据
1	需要使能 SSM Mapping 功能的接口
3	组播组地址和掩码、组播源地址和掩码

3.6.2 使能 SSM Mapping 功能

在与用户网段相连的组播设备接口使能 SSM Mapping 是配置 SSM Mapping 功能的首要步骤。

背景信息

在配置静态 SSM Mapping 策略之前，要先使能 SSM Mapping 功能。只有在接口上使能 SSM Mapping，配置的 SSM 源组地址映射表项才能生效。

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 **igmp enable**，使能 IGMP 功能。

步骤 4 执行命令 **igmp version 3**，配置 IGMP 版本号为 3。为保证该网段内运行任意版本 IGMP 的用户主机都能得到 SSM 服务，建议在路由器接口上运行 IGMPv3。

步骤 5 执行命令 **igmp ssm-mapping enable** ，使能 SSM Mapping 功能。

----结束

3.6.3 配置静态 SSM Mapping 策略

在与用户网段相连的组播设备上配置 SSM Mapping 功能，使只支持 IGMPv1 或 IGMPv2、不支持 IGMPv3 的用户主机可以加入指定源组，达到高版本组播设备兼容低版本主机并向这些用户提供 SSM 服务的目的。

背景信息

配置静态 SSM Mapping 策略可以让使能了 SSM Mapping 功能的接口按照配置的映射策略进行组到源的映射，从而使高版本组播设备兼容低版本主机并向这些用户提供 SSM 服务。

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 **igmp** [**vpn-instance** *vpn-instance-name*]，进入 IGMP 视图。

步骤 3 执行命令 **ssm-mapping** *group-address* { *mask* | *mask-length* } *source-address*，配置组到源的映射。多次配置，可以实现同一个组到多个源的映射。

- *group-address* { *mask* | *mask-length* }为组地址和掩码。
- *source-address* 为与组建立映射关系的源地址。

----结束

3.6.4 检查配置结果

配置 SSM Mapping 成功后，查看用于 SSM Mapping 的组信息、特定组地址的 SSM Mapping 映射规则、以及接口上是否使能了 SSM Mapping，确保 SSM Mapping 正常运行。

操作步骤

- 使用 **display igmp group** [*group-address* | **interface** *interface-type interface-number*] * **ssm-mapping** [**verbose**]命令查看用于 SSM Mapping 的组信息。
- 使用 **display igmp ssm-mapping group** [*group-address*]命令查看特定组地址的 SSM Mapping 映射规则。
- 使用 **display igmp ssm-mapping interface** [*interface-type interface-number*]命令查看接口上是否使能了 SSM Mapping。

----结束

3.7 配置 IGMP Limit 功能

当运营商希望限制可服务的 IPTV ICP 及用户接入的数量时，可配置 IGMP Limit 功能。IGMP Limit 功能包括：全局 IGMP 组成员关系个数限制、单实例 IGMP 全局表项限制和基于接口的 IGMP组成员关系个数限制。

3.7.1 建立配置任务

在配置 IGMP Limit 功能前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以快速、准确地完成配置任务。

应用环境

IGMP Limit 功能可用于 IPv4 PIM-SM 和 IPv4 PIM-DM 网络中。

当运营商希望限制可服务的 IPTV ICP（Internet Content Provider，Internet 内容提供商）、控制用户接入的数量时，可以配置 IGMP Limit 功能。

IGMP Limit 功能在连接用户的最后一跳路由器上配置，用户可以根据实际需求选择以下配置。

- 配置全局 IGMP 组成员关系个数限制
- 配置单实例 IGMP 全局表项限制
- 配置基于接口的 IGMP 组成员关系个数限制

说明

若需要在同一路由器上配置基于全局、单实例和接口的 IGMP Limit 功能时，建议全局 IGMP 组成员关系个数限制值>单实例 IGMP 组成员关系个数限制值>基于接口 IGMP 组成员关系个数限制值。

前置任务

在配置 IGMP Limit 功能之前，需完成以下任务：

- 配置某单播路由协议，使整个组播域连通
- **配置 IGMP 的基本功能**

数据准备

在配置 IGMP Limit 功能之前，需要准备以下数据。

序号	数据
1	全局 IGMP 组成员关系个数限制值
2	单实例 IGMP 组成员关系个数限制值
3	基于接口 IGMP 组成员关系个数限制值

3.7.2 配置全局 IGMP 组成员关系个数限制

在与用户网段相连的组播设备上配置可创建的 IGMP 表项的最大个数。当 IGMP 表项个数达到限制值后，将不再创建 IGMP 表项。若需要加入新的组播组，建议删除一些无用的表项、修改限制值、或加入静态组播组/源组。

背景信息

在与用户主机相连的路由器上进行如下配置。

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 **igmp global limit** *number*，配置所有实例 IGMP 全局表项限制。

----结束

3.7.3 配置单实例 IGMP 全局表项限制

在与用户网段相连的组播设备上配置单实例可创建的 IGMP 表项的最大个数。当 IGMP 表项个数达到限制值后，将不再创建 IGMP 表项。若需要加入新的组播组，建议删除一些无用的表项、修改限制值，或加入静态组播组/源组。

背景信息

在与用户主机相连的路由器上进行如下配置。

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 **igmp**，进入 IGMP 视图。

步骤 3 执行命令 **limit** *number*，配置单实例 IGMP 全局表项限制。

----结束

3.7.4 配置基于接口的 IGMP 组成员关系个数限制

在与用户网段相连的组播设备接口上配置可创建的 IGMP 表项的最大个数。当 IGMP 表项个数达到限制值后，将不再创建 IGMP 表项。若需要加入新的组播组，建议删除一些无用的表项、修改限制值、或加入静态组播组/源组。

背景信息

在与用户主机相连的路由器上进行如下配置。

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 IGMP 接口视图。

步骤 3 执行命令 **igmp limit** *number* [**except** { *acl-number* | **acl-name** *acl-name* }]，配置当前接口上能够创建的 IGMP 组成员关系最大个数。

说明

- 如果未使用 **except** 参数，则动态创建的所有组或源组时都受 IGMP 表项最大个数的限制。
- 使用 **except** 参数之前，需要配置相应的 ACL，接口将按照该 ACL 过滤收到的 IGMP 加入报文。创建通过 ACL 过滤的表项时不受 IGMP 表项最大个数限制。

----结束

3.7.5 检查配置结果

配置 IGMP Limit 成功后，查看接口上的 IGMP 配置和运行信息、以及 IGMP 组播组的成员信息，确保 IGMP 正常运行。

操作步骤

- 执行 **display igmp interface** [*interface-type interface-number* | **up** | **down**] [**verbose**] 命令查看接口上的 IGMP 配置和运行信息。
- 执行以下命令查看 IGMP 组播组的成员信息：
  - **display igmp group** [*group-address* | **interface** *interface-type interface-number*] * [**verbose**]
  - **display igmp group** [*group-address* | **interface** *interface-type interface-number*] * **ssm-mapping** [**verbose**]

----结束

任务示例

使用 **display igmp interface** 命令查看路由器接口上 IGMP 的配置和运行情况。显示信息如下：

```
<RouterA> display igmp interface gigabitethernet 1/0/0
Interface information
 GigabitEthernet1/0/0(10.2.1.1):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: 40
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Querier for IGMP: 10.2.1.1 (this router)
```

可以看到 RouterA 的 GigabitEthernet1/0/0 上可创建的 IGMP 组成员关系的最大个数。

3.8 维护 IGMP

IGMP 的维护包括：清除 IGMP 的组信息。

3.8.1 清除 IGMP 的组信息

在确认需要清除 IGMP 的组信息后，在用户视图下选择执行 reset 命令,清除 IGMP 的组信息。删除接口上动态加入的 IGMP 组播组时，可能导致接收者无法正常接收组播信息，请慎用。

背景信息

注意

执行 **reset igmp group** 或 **reset igmp group ssm-mapping** 命令将删除接口上已经动态加入的 IGMP 组，可能导致接收者无法正常接收组播信息，请慎用。

操作步骤

- 在确认需要清除接口上已经动态加入的 IGMP 组后，请在用户视图下执行 **reset igmp group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *group-mask* | *group-mask-length* }] [*source-address* [**mask** { *source-mask* | *source-mask-length* }]] } }命令。
- 在确认需要清除接口上已经静态加入的 IGMP 组后，请在接口视图下执行 **undo igmp static-group** { **all** | *group-address* [**inc-step-mask** { *group-mask* | *group-mask-length* } **number** *group-number*] [**source** *source-address*] }命令。
- 在确认需要清除配置了 SSM 映射的组播组信息后，请在用户视图下执行 **reset igmp group ssm-mapping** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *group-mask* | *group-mask-length* }] } }命令。
- 在确认需要清除接口上通过 IGMP 动态加入组播组的主机后，请在用户视图下执行 **reset igmp explicit-tracking** { **all** | **interface** *interface-type interface-number* [**host** *host-address* [**group** *group-address* [**source** *source-address*]]] }命令。
- 在确认需要清除 IGMP 消息统计数后，请在用户视图下执行 **reset igmp control-message counters** [**interface** *interface-type interface-number*] [**message-type** { **query** | **report** }]命令。

----结束

3.9 配置举例

针对如何在组播网络中配置 IGMP 基本功能、SSM-Mapping、以及 IGMP Limit，分别提供配置举例。

3.9.1 配置 IGMP 的基本功能示例

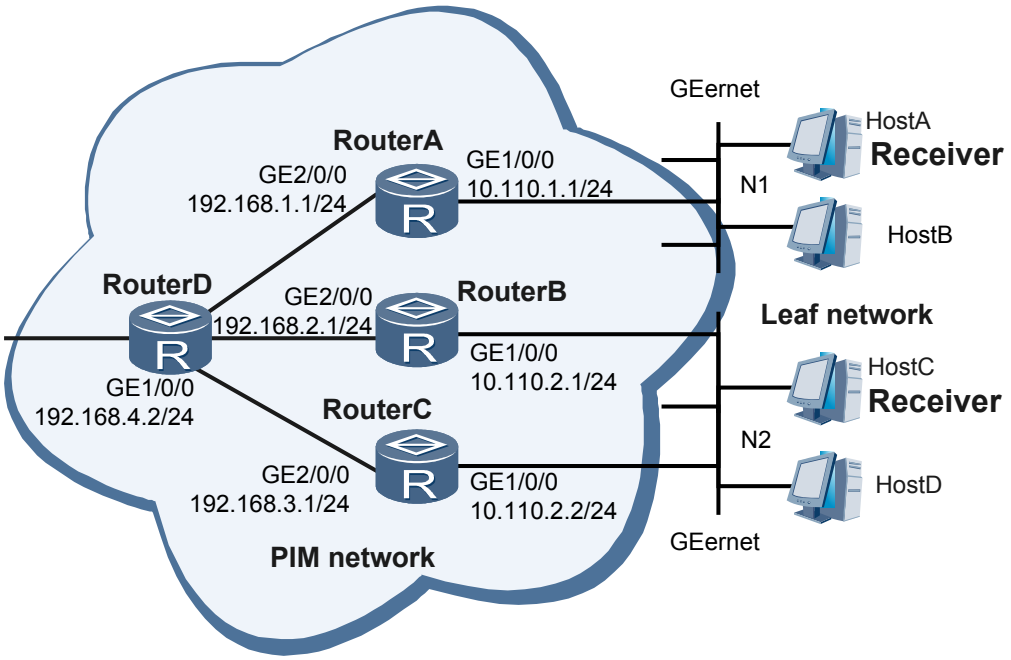
在组播网络中部署 IGMP 基本功能，实现用户主机长期稳定接收组播源发送的组播数据。

组网需求

如图 3-1 所示的 IPv4 网络中，单播路由正常。要求在该网络中部署组播功能，使用户主机能够接收视频点播信息。

当路由器某个接口下的用户需要长期接收热点节目时，将该接口静态加入组播组。如下网络中，Host A 和 Host B 需要长期接收组播组 225.1.1.1 的数据，则将路由器接口 GE1/0/0 配置成静态加入组播组 225.1.1.1。

图 3-1 配置 IGMP 的基本功能组网图



配置思路

采用如下的思路配置 IGMP 的基本功能：

1. 在所有为组播服务的路由器上使能组播功能。组播功能是 IGMP 功能的前提条件。
2. 在所有组播路由器接口上使能 PIM-SM 功能。
3. 在连接用户主机的组播路由器接口上使能 IGMP 功能。
4. 将 RouterA 的 GE1/0/0 接口静态加入组播组 225.1.1.1，长期稳定地接收组 225.1.1.1 的数据。

数据准备

为完成此配置举例，需准备如下的数据：

- 静态 RP 地址为 192.168.4.1。
- 静态组播组地址为 225.1.1.1。

操作步骤

步骤 1 配置各 Router 接口 IP 地址和单播路由协议

按照图 3-1 配置各接口的 IP 地址和掩码，并配置各 Router 之间采用 OSPF 进行互连，确保网络中各 Router 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。具体配置过程略，详见配置文件。

步骤 2 配置 PIM-SM 功能和配置静态 RP

在 RouterA 上使能组播功能，并在 GE 1/0/0 接口上使能 PIM-SM 功能。RouterB、RouterC 和 RouterD 上的配置过程与此完全相同，配置过程略，详见配置文件。

```
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] pim sm
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] pim
[RouterA-pim] static-rp 192.168.4.1
[RouterA-pim] quit
```

步骤 3 在主机侧接口上使能 IGMP 功能

在 RouterA 的 GE1/0/0 接口上使能 IGMP 功能。RouterB 和 RouterC 配置过程与此完全相同，配置过程略，详见配置文件。

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

步骤 4 将 RouterA 的 GE1/0/0 接口静态加入组播组 225.1.1.1，使接口 GE1/0/0 下的用户能长期接收发往组播 225.1.1.1 的数据

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] igmp static-group 225.1.1.1
```

步骤 5 验证配置结果

通过使用 **display igmp interface** 命令可以查看各路由器接口上 IGMP 的配置和运行情况。例如 RouterB 的 GE1/0/0 接口上 IGMP 的显示信息如下：

```
<RouterB> display igmp interface gigabitethernet 1/0/0
Interface information
 GigabitEthernet1/0/0(10.110.2.1):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP(configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Querier for IGMP: 10.110.2.1 (this router)
  Total 2 IGMP Groups reported
```

在 RouterA 上通过使用命令 **display pim routing-table** 可以查看，接口 GE1/0/0 是否静态加入组播组 225.1.1.1。显示信息如下，如果 RouterA 上，有（*，225.1.1.1）表项，且下游接口是 GigabitEthernet1/0/0，协议类型为“static”，则表明 GigabitEthernet1/0/0 静态加入组播组 225.1.1.1 配置成功。

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

 (*, 225.1.1.1)
     RP: 192.168.4.1
     Protocol: pim-sm, Flag: WC
     UpTime: 00:12:17
     Upstream interface: GigabitEthernet2/0/0
         Upstream neighbor: 192.168.1.1
         RPF prime neighbor: 192.168.1.1
     Downstream interface(s) information:
     Total number of downstreams: 1
```

```
    1: GigabitEthernet1/0/0
        Protocol: static, UpTime: 00:12:17, 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
 igmp enable
 igmp static-group 225.1.1.1
#
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
#
pim
 static-rp 192.168.4.1
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.110.2.1 255.255.255.0
 pim sm
 igmp enable
#
interface GigabitEthernet2/0/0
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
pim
 static-rp 192.168.4.1
#
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 192.168.4.1
#
return
```

3.9.2 配置 SSM Mapping 功能示例

用户主机只能运行 IGMPv1 或 IGMPv2，不能升级到 IGMPv3，在组播网络中部署 SSM-Mapping，实现高版本组播设备兼容低版本主机并向这些用户提供 SSM 服务，用户主机能够接收到指定组播源发送的组播数据。

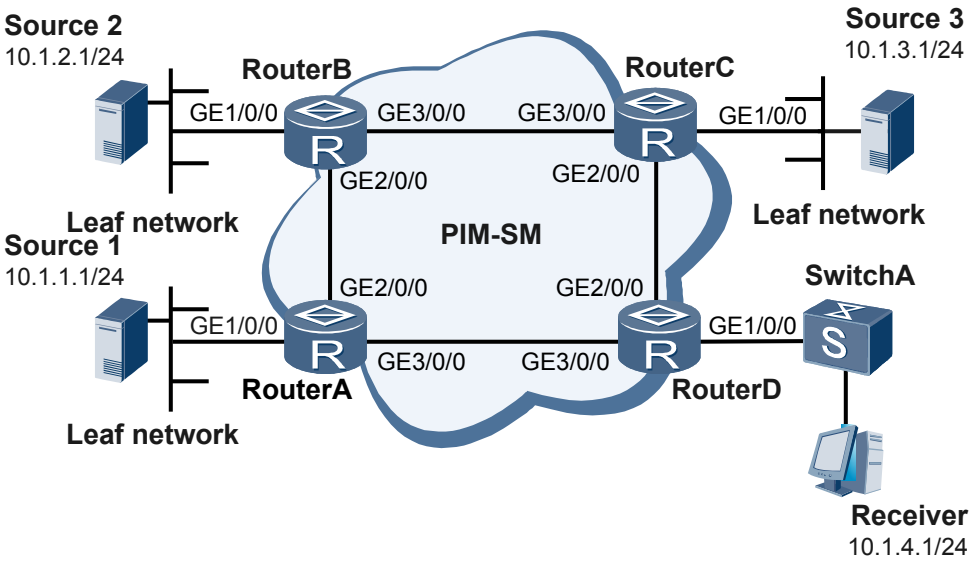
组网需求

如图 3-2 所示的组播网络中，运行 PIM-SM 协议，同时 SSM 模式提供组播服务。与用户主机 Receiver 相连的路由器接口上运行 IGMPv3，Receiver 上的 IGMP 的版本为 v2，不能升级到 IGMPv3。

当前网络中的 SSM 组地址范围是 225.1.1.0/24，Source 1、Source 2 和 Source 3 都向该范围内的组播组发送组播数据。用户期望只接收来自 Source 1 和 Source 3 的组播数据。

解决方案：在 RouterD 上进行 SSM Mapping 功能配置。

图 3-2 配置 SSM Mapping 功能组网图



Device	接口	IP 地址	Device	接口	IP 地址
Router A	GE 1/0/0	10.1.1.2/24	Router C	GE 1/0/0	10.1.3.2/24
	GE 2/0/0	192.168.1.1/24		GE 2/0/0	192.168.3.1/24
	GE 3/0/0	192.168.4.2/24		GE 3/0/0	192.168.2.2/24
Router B	GE 1/0/0	10.1.2.2/24	Router D	GE 1/0/0	10.1.4.2/24

GE 2/0/0	192.168.1.2/24	GE 2/0/0	192.168.3.2/24
GE 3/0/0	192.168.2.1/24	GE 3/0/0	192.168.4.1/24

配置思路

采用如下的思路配置 SSM Mapping 功能：

1. 在连接用户主机的组播路由器接口上使能 SSM Mapping 功能；
2. 在该 PIM-SM 域内的所有组播路由器上配置 SSM 组播组地址范围；
3. 在使能了 SSM Mapping 功能的路由器上配置 SSM Mapping 静态映射规则。

数据准备

为完成此配置举例，需准备如下的数据：

- SSM 组播组范围
- Source 1 和 Source 3 的 IP 地址

操作步骤

步骤 1 配置各 Router 接口 IP 地址和单播路由协议

按照图 3-2 配置各接口的 IP 地址和掩码，并配置各 Router 之间采用 OSPF 进行互连，确保网络中各 Router 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。具体配置过程略，详见配置文件。

步骤 2 在连接用户主机的接口上使能 IGMP 功能和 SSM Mapping 功能

```
[RouterD] multicast routing-enable
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] igmp enable
[RouterD-GigabitEthernet1/0/0] igmp version 3
[RouterD-GigabitEthernet1/0/0] igmp ssm-mapping enable
[RouterD-GigabitEthernet1/0/0] quit
```

步骤 3 配置 SSM 组播组地址范围

在所有路由器上配置 SSM 组播组地址范围为 225.1.1.0/24。RouterB、RouterC 和 RouterD 上的配置过程与 RouterA 上的配置完全相同，配置过程略，详见配置文件。

```
[RouterA] acl number 2000
[RouterA-acl-basic-2000] rule permit source 225.1.1.0 0.0.0.255
[RouterA-acl-basic-2000] quit
[RouterA] pim
[RouterA-pim] ssm-policy 2000
```

步骤 4 在连接用户主机的路由器上配置 SSM Mapping 静态映射规则

将 225.1.1.0/24 范围内的组播组映射到 Source 1 和 Source 3。

```
[RouterD] igmp
[RouterD-igmp] ssm-mapping 225.1.1.0 24 10.1.1.1
[RouterD-igmp] ssm-mapping 225.1.1.0 24 10.1.3.1
```

查看路由器上特定源/组地址的 SSM Mapping 信息。

```
<RouterD> display igmp ssm-mapping group
IGMP SSM-Mapping conversion table
```

```
 Total 2 entries    2 entries matched
 00001. (10.1.1.1, 225.1.1.0)
 00002. (10.1.3.1, 225.1.1.0)
 Total 2 entries matched
```

步骤 5 验证配置结果

Receiver 加入组 225.1.1.1。

通过使用 **display igmp group ssm-mapping** 命令，可以查看路由器上特定源/组地址的信息。RouterD 上特定源/组地址信息显示如下：

```
<RouterD> display igmp group ssm-mapping
IGMP SSM mapping interface group report information
 GigabitEthernet1/0/0 (10.1.4.2):
  Total 1 IGMP SSM-Mapping Group reported
   Group Address   Last Reporter   Uptime      Expires
   225.1.1.1       10.1.4.1     00:01:44    00:00:26
<RouterD> display igmp group ssm-mapping verbose
Interface group report information
 Limited entry of this VPN-Instance: -
 GigabitEthernet1/0/0 (10.1.4.2):
  Total entry on this interface: 1
  Limited entry on this interface: -
  Total 1 IGMP SSM-Mapping Group reported
   Group: 225.1.1.1
     Uptime: 00:01:52
     Expires: 00:00:18
     Last reporter: 10.1.4.1
     Last-member-query-counter: 0
     Last-member-query-timer-expiry: off
     Group mode: exclude
     Version1-host-present-timer-expiry: off
     Version2-host-present-timer-expiry: 00:00:17
```

通过使用 **display pim routing-table** 命令，可以查看路由器 PIM-SM 组播路由表。RouterD 上 PIM-SM 组播路由表信息显示如下：

```
<RouterD> display pim routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 2 (S, G) entries
 (10.1.1.1, 225.1.1.1)
     Protocol: pim-ssm, Flag:SG_RCVR
     UpTime: 00:11:25
     Upstream interface: GigabitEthernet3/0/0
         Upstream neighbor: 192.168.4.2
         RPF prime neighbor: 192.168.4.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/0
             Protocol: ssm-map, UpTime: 00:11:25, Expires:-
 (10.1.3.1, 225.1.1.1)
     Protocol: pim-ssm, Flag:SG_RCVR
     UpTime: 00:11:25
     Upstream interface: GigabitEthernet2/0/0
         Upstream neighbor: 192.168.3.1
         RPF prime neighbor: 192.168.3.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/0
             Protocol: ssm-map, UpTime: 00:11:25, Expires:-
```

----结束

配置文件

- RouterA 的配置文件

```
#
```

```
 sysname RouterA
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 225.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 192.168.4.2 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.4.0 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 225.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 10.1.2.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 192.168.1.0 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 225.1.1.0 0.0.0.255
```

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.3.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.1.3.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- RouterD 的配置文件

```
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 225.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 10.1.4.2 255.255.255.0
 pim sm
 igmp enable
 igmp version 3
 igmp ssm-mapping enable
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 192.168.4.1 255.255.255.0
 pim sm
#
igmp
 ssm-mapping 225.1.1.0 255.255.255.0 10.1.1.1
 ssm-mapping 225.1.1.0 255.255.255.0 10.1.3.1
#
pim
 ssm-policy 2000
#
return
```

3.9.3 配置 IGMP Limit 示例

在组播网络中与用户网段相连的组播设备上配置 IGMP Limit，在用户侧实现对 IGMP 组成员关系的数量限制，使运营商能够灵活控制组播网络。

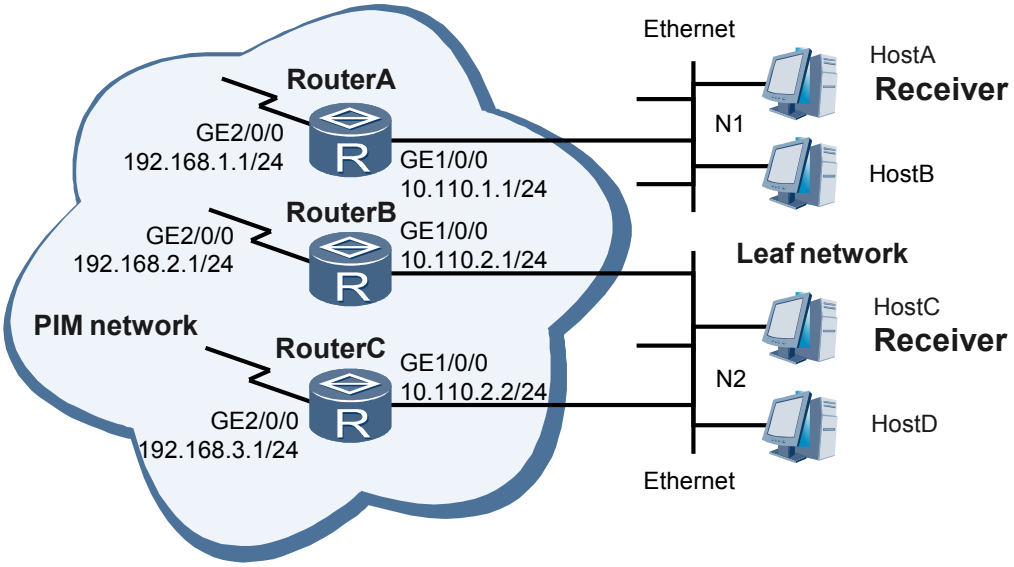
组网需求

大量用户同时收看多套视频节目时，要占用设备的大量带宽，造成设备性能下降，导致用户接收组播数据的稳定性变差。

在已有的组播技术中，通过限制组播转发表表项数量或限制组播转发表单个表项的出接口数量控制组播网络，此方案不能满足运营商对 IPTV 网络中承载的实时视频业务及可用的网络资源进行灵活管理的要求。

通过配置 IGMP 组成员关系限制，可以使运营商合理规划网络资源，灵活控制用户能够接入的组播组数量。如图 3-3 所示的网络中部署组播业务，在与用户主机相连的设备 RouterA、RouterB 和 RouterC 上配置基于全局、单实例、和接口的 IGMP 组成员关系限制，限制用户能够加入的组播组数量，当达到限制值时不允许创建新的 IGMP 表项，保证已经加入组播组的用户收看更加清晰稳定的节目。

图 3-3 配置 IGMP Limit 组网图



配置思路

采用如下的思路配置 IGMP Limit 的基本功能：

1. 在所有为组播服务的路由器上使能组播功能。组播功能是 IGMP 功能的前提条件。
2. 在所有组播路由器接口上使能 PIM-SM 功能。
3. 在连接用户主机的组播路由器接口上使能 IGMP 功能。
4. 将 RouterA 的 GE1/0/0 接口静态加入组播组 225.1.1.1，长期稳定地接收组 225.1.1.1 的数据。
5. 在 RouterA 上配置 IGMP 组成员关系个数限制。

数据准备

为完成此配置举例，需准备如下的数据：

- 路由器与用户主机之间运行的 IGMP 版本号。
- 静态组播组地址：225.1.1.1。
- IGMP 组成员关系个数限制值。

操作步骤

步骤 1 配置各 Router 接口 IP 地址和单播路由协议。

按照图 3-3 配置各接口的 IP 地址和掩码，并配置各 Router 之间采用 OSPF 进行互连，确保网络中各 Router 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。具体配置过程略，详见配置文件。

步骤 2 使能组播功能，并在主机侧接口上使能 IGMP 功能和 PIM-SM 功能

在 RouterA 上使能组播功能，并在 GE1/0/0 接口上使能 IGMP 功能和 PIM-SM 功能，配置 IGMP 版本为 v2。RouterB 和 RouterC 上的配置与 RouterA 类似，配置过程略，详见配置文件。

```
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] pim sm
[RouterA-GigabitEthernet1/0/0] igmp enable
[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 将 RouterA 的 GE1/0/0 接口静态加入组播组 225.1.1.1，使接口 GE1/0/0 下的用户能长期接收发往组播 225.1.1.1 的数据

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] igmp static-group 225.1.1.1
[RouterA-GigabitEthernet1/0/0] quit
```

步骤 4 在连接用户的最后一跳路由器上配置 IGMP 组成员关系个数限制

配置 RouterA 上总共可以创建 50 个 IGMP 组成员关系。

```
[RouterA] igmp global limit 50
```

配置公网实例下总共可以创建 40 个 IGMP 组成员关系。

```
[RouterA] igmp
[RouterA-igmp] limit 40
[RouterA-igmp] quit
```

配置接口 GE1/0/0 下总共可以创建 30 个 IGMP 组成员关系。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] igmp limit 30
[RouterA-GigabitEthernet1/0/0] quit
```

RouterB 和 RouterC 上的配置与 RouterA 类似，配置过程略。

步骤 5 验证配置结果

通过使用 **display igmp interface** 命令可以查看路由器接口上 IGMP 的配置和运行情况。RouterA 的 GE1/0/0 接口上 IGMP 的显示信息如下：

```
<RouterA> display igmp interface gigabitethernet 1/0/0
Interface information
 GigabitEthernet1/0/0(10.110.1.1):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: 30
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
```

```
Value of maximum query response time for IGMP: 10 s
Querier for IGMP: 10.110.1.1 (this router)
```

可以看到，RouterA 的 GE1/0/0 上可创建的 IGMP 组成员关系的最大个数为 30 个。

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 igmp global limit 50
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.110.1.1 255.255.255.0
 pim sm
 igmp enable
 igmp limit 30
 igmp static-group 225.1.1.1
#
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
#
igmp
 limit 40
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 igmp global limit 50
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.110.2.1 255.255.255.0
 pim sm
 igmp enable
 igmp limit 30
#
interface GigabitEthernet2/0/0
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
igmp
 limit 40
#
return
```

- RouterC 的配置文件

```
#
```

```
 sysname RouterC
#
 igmp global limit 50
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.110.2.2 255.255.255.0
 pim sm
 igmp enable
 igmp limit 30
#
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
#
igmp
 limit 40
#
return
```

4 PIM-DM（IPv4）配置

关于本章

通过配置 PIM 协议，可以实现 AS 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密集的小型网络。

4.1 PIM-DM 概述
在组成员分布非常稠密，每个网段都可能存在组成员的网络中，PIM-DM 通过周期性的“扩散—剪枝”，构建并维护一棵连接组播源和组成员的单向无环 SPT。

4.2 AR2200-S 支持的 PIM-DM 特性
系统采用 PIM-DM 的缺省值可以正常工作，允许用户根据具体环境适当调整邻居、剪枝、状态刷新、嫁接和 Assert 等相关参数，通过配置各种过滤策略和 PIM Silent 功能来提高 PIM-DM 的安全性。

4.3 配置 PIM-DM 基本功能
在单播路由畅通的情况下，在每台设备上使能 IPv4 组播路由，在设备的每个接口上使能 PIM-DM，PIM-DM 网络就可以正常运行了。

4.4 调整组播源控制参数
设备可以基于组播源来控制组播报文的转发。一方面有助于数据流量控制，另一方面可以限定下游接收者能够获得的信息，提高安全性。

4.5 调整邻居控制参数
设备间通过交互 Hello 消息建立 PIM 邻居关系，协商各类控制参数，通过 Hello 消息中携带的控制参数来控制邻居关系。

4.6 调整剪枝控制参数
当下游接口上最后一个组成员离开时，设备的上游接口发送 Prune 消息请求上游设备执行剪枝，同网段其他仍需要该组数据的下游设备必须发送 Join 消息来否决剪枝。

4.7 调整状态刷新控制参数
周期性的“扩散-剪枝”将造成很大的网络资源浪费。为防止被剪枝接口因为剪枝状态超时而恢复转发，系统启用了状态刷新功能，周期性的发送 State-Refresh 消息，刷新接口剪枝状态，维持 SPT 树。

4.8 调整嫁接控制参数
为使网络中出现的新的组成员能够快速的接收到组播数据，设备会主动从上游接口发出 Graft 消息，请求上游设备向该网段转发组播数据。

4.9 调整 Assert 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 消息，参与竞选唯一上游。

4.10 配置防止主机恶意攻击功能（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。

4.11 维护 PIM-DM（IPv4）

PIM-DM 的维护包括：清除 PIM 统计信息。

4.12 配置举例

通过配置举例，可以了解如何构建基本的 PIM-DM 网络。

4.1 PIM-DM 概述

在组成员分布非常稠密，每个网段都可能存在组成员的网络中，PIM-DM 通过周期性的“扩散—剪枝”，构建并维护一棵连接组播源和组成员的单向无环 SPT。

注意

本章只关注 IPv4 组播网络中 PIM-DM 的配置。

PIM（Protocol Independent Multicast）称为协议无关组播，表示为 IP 组播提供路由信息的可以是静态路由、RIP、OSPF、IS-IS、BGP 等任何一种单播路由协议。组播路由和单播路由协议无关，只要通过单播路由协议能够产生相应组播路由表项即可。

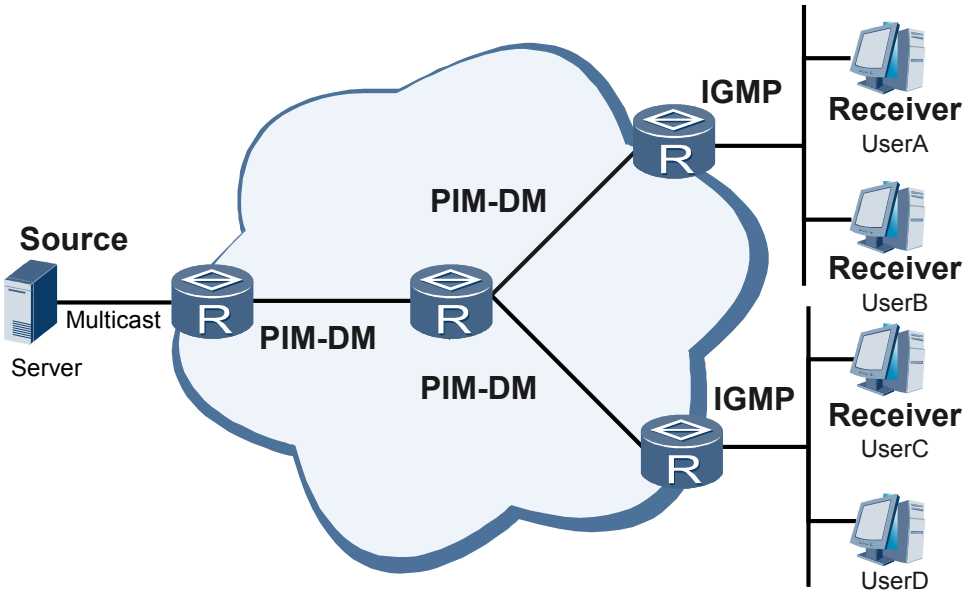
PIM 借助 RPF（Reverse Path Forwarding）机制实现组播报文转发。RPF 机制利用现存的单播路由信息在网络中构建组播转发树。当一个组播报文到达路由器时，首先进行 RPF 检查。如果 RPF 检查失败，则将该报文丢弃。

说明

关于 RPF 的详细说明请参见 **7 IPv4 组播路由管理**。

PIM-DM（Protocol Independent Multicast Dense Mode）称为协议独立组播－密集模式，属于密集模式的组播路由协议，适用于组成员分布相对密集的小型网络。PIM-DM 在组播网络中的作用和位置如图 4-1 所示。

图 4-1 PIM-DM 在组播网络中的应用示意图



对于组成员分布相对分散、范围较广、大规模的网络适用 PIM-SM（Protocol Independent Multicast-Sparse Mode）。有关 PIM-SM 的配置方法，请参见 **5 PIM-SM（IPv4）配置**。

4.2 AR2200-S 支持的 PIM-DM 特性

系统采用 PIM-DM 的缺省值可以正常工作，允许用户根据具体环境适当调整邻居、剪枝、状态刷新、嫁接和 Assert 等相关参数，通过配置各种过滤策略和 PIM Silent 功能来提高 PIM-DM 的安全性。

说明

异步串口，ISDN BRI 接口，3G 接口，Bridge-if 接口，NULL 接口，QinQ 子接口不支持 PIM-DM。

控制组播源转发

用户可以配置组播源生存时间和组播源的过滤规则。

调整邻居控制参数

用户可以调整以下邻居控制参数：

- 发送 Hello 消息的时间间隔。
- 保持邻居为可达状态的超时时间。
- 是否接收不包含 Generation ID 选项的 Hello 消息。
- 触发 Hello 消息的最大时延。
- 邻居过滤功能。接口只与符合过滤规则的地址建立邻居关系，删除不符合过滤规则的邻居。

调整剪枝控制参数

用户可以调整以下参数：

- 下游接口保持剪枝状态的时间间隔。
- 在 LAN 内，当前路由器从接收到下游发送的剪枝消息到开始实施剪枝动作的延迟时间。
- 否决剪枝时间。

调整状态刷新控制参数

用户可以禁止或使能状态刷新功能、配置发送 PIM 状态刷新消息的时间间隔、配置接收下一个状态刷新消息的最小时间间隔、在源直连路由器上配置转发状态刷新消息的 TTL 值。

调整嫁接控制参数

用户可以调整重传 Graft 消息的时间间隔。

调整 Assert 控制参数

用户可以调整路由器保持 Assert 状态的时间，落选路由器在此时间内禁止下游接口转发组播数据，超时后恢复转发。

防止主机恶意攻击功能

用户主机发送大量恶意的 PIM Hello 报文可能导致路由器瘫痪。在与用户相连的接口上配置 PIM Silent 功能，可以防止路由器受到攻击。

4.3 配置 PIM-DM 基本功能

在单播路由畅通的情况下，在每台设备上使能 IPv4 组播路由，在设备的每个接口上使能 PIM-DM，PIM-DM 网络就可以正常运行了。

4.3.1 建立配置任务

在配置 PIM-DM 基本功能之前，需配置 IPv4 单播路由协议。

应用环境

PIM-DM 适用于规模较小且网络中绝大多数网段都存在接收者的网络。

前置任务

在配置 PIM-DM 基本功能之前，需配置 IPv4 单播路由协议。

数据准备

在配置 PIM-DM 基本功能之前，需准备以下数据。

序号	数据
1	欲启动 PIM-DM 功能的接口类型和编号

4.3.2 使能 IPv4 组播路由

使能 IPv4 组播路由是配置所有 IPv4 组播特性的首要步骤。

背景信息

在路由器上进行如下配置。

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 **multicast routing-enable**，使能公网实例 IP 组播路由。

----结束

4.3.3 使能 PIM-DM 功能

接口上使能了 PIM-DM 后，才可以和其他设备建立 PIM 邻居。

背景信息

说明

同一接口上不能同时使能 PIM-DM 和 PIM-SM 功能，而且路由器上属于同一实例的所有接口的 PIM 模式必须相同。当路由器被部署在 PIM-DM 域中时，建议在全部非边界接口上使能 PIM-DM 功能。

在路由器上进行如下配置。

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 dm**，使能 PIM-DM 功能。在接口上使能了 PIM-DM 功能后，路由器之间建立 PIM 邻居，从而才能对来自 PIM 邻居的协议报文进行处理。

----结束

4.3.4 检查配置结果

配置 PIM-DM 基本功能成功后，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 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看公网实例接口上的 PIM 信息。
- 使用 **display pim neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *命令查看公网实例的 PIM 邻居信息。
- 使用以下命令查看公网实例的 PIM 协议组播路由表：
  - **display pim 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 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

任务示例

执行 **display pim interface verbose** 命令，查看公网实例下接口上的 PIM 详细信息。

```
<Huawei> display pim interface verbose
 VPN-Instance: public net
 Interface: GigabitEthernet0/0/2, 10.1.2.2
     PIM version: 2
     PIM mode: Sparse
     PIM state: up
     PIM DR: 10.1.2.2 (local)
     PIM DR Priority (configured): 1
     PIM neighbor count: 0
```

```
    PIM hello interval: 30 s
    PIM LAN delay (negotiated): 500 ms
    PIM LAN delay (configured): 500 ms
    PIM hello override interval (negotiated): 2500 ms
    PIM hello override interval (configured): 2500 ms
    PIM Silent: disabled
    PIM neighbor tracking (negotiated): disabled
    PIM neighbor tracking (configured): disabled
    PIM generation ID: 0X4B9F5B92
    PIM require-GenID: disabled
    PIM hello hold interval: 105 s
    PIM assert hold interval: 180 s
    PIM triggered hello delay: 5 s
    PIM J/P interval: 60 s
    PIM J/P hold interval: 210 s
    PIM BSR domain border: disabled
    PIM BFD: disabled
    PIM dr-switch-delay timer : not configured
    Number of routers on link not using DR priority: 0
    Number of routers on link not using LAN delay: 0
    Number of routers on link not using neighbor tracking: 1
    ACL of PIM neighbor policy: -
    ACL of PIM ASM join policy: -
    ACL of PIM SSM join policy: -
    ACL of PIM join policy: -
```

执行 **display pim neighbor verbose** 命令，查看公网实例下 PIM 邻居的详细信息。

```
<Huawei> display pim neighbor verbose
 VPN-Instance: public net
 Total Number of Neighbors = 1

 Neighbor: 50.1.1.2
     Interface: Vlanif50
     Uptime: 00:41:32
     Expiry time: 00:01:43
     DR Priority: 1
     Generation ID: 0XF263678D
     Holdtime: 105 s
     LAN delay: 500 ms
     Override interval: 2500 ms
     Neighbor tracking: Disabled
     PIM BFD-Session: N
```

4.4 调整组播源控制参数

设备可以基于组播源来控制组播报文的转发。一方面有助于数据流量控制，另一方面可以限定下游接收者能够获得的信息，提高安全性。

4.4.1 建立配置任务

配置 PIM-DM 基本功能后，可以根据实际需要配置源生存时间和源地址过滤规则。

应用环境

此配置在所有应用 PIM-DM 的网络中均适用。

PIM 路由器对流经自己的组播数据进行检查，通过比较是否符合过滤规则，判断组播报文是否继续转发。这时，可以将路由器看作组播数据的过滤器。过滤器的存在一方面有助于实现数据流量控制，另一方面可以在安全性方面限定下游接收者能够获得的信息。

前置任务

在控制组播源转发之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-DM 基本功能**

数据准备

在控制组播源转发之前，需准备以下数据。

序号	数据
1	组播源生存时间
2	组播源地址过滤规则

4.4.2 配置源生存时间

设备为每个(S,G)表项建立一个定时器。如果设备在“源生存时间”内没有收到 S 发出的组播报文，则认为(S,G)表项失效，组播源停止向组 G 发送组播数据。

背景信息

在 PIM 路由器上进行如下配置。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

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** ，进入 PIM 视图。

步骤 3 执行命令 **source-lifetime** *interval*，配置组播源生存时间，如果路由器在“组播源生存时间”之内没有收到（S，G）报文，则认为（S，G）表项失效，组播源停止向组 G 发送组播数据。

在使能了状态刷新的情况下，组播源生存时间会延长 *interval* 参数定义的时间。

----结束

4.4.3 配置源地址过滤规则

通过配置 ACL 规则，设备会根据源地址或源/组地址过滤接收的组播报文。

背景信息

在 PIM 路由器上进行如下配置。

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** ，进入 PIM 视图。

步骤 3 执行命令 **source-policy** { *acl-number* | **acl-name** *acl-name* }，配置过滤器。设置过滤器的位置离组播源距离越近，过滤效果越明显。

- 如果配置的是基本 ACL，则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，则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。

说明

- 如果配置 *acl-number* | **acl-name** *acl-name* 的过滤规则，采用 **source-policy** 命令可以转发源地址属于过滤规则允许范围的组播报文。
- 如果仅指定 *acl-number* | **acl-name** *acl-name*，不配置其过滤规则，采用 **source-policy** 命令不转发任何源地址发送的组播报文。
- **source-policy** 命令不过滤静态（S，G）和记录了私网加入信息的 PIM 表项。

----结束

4.4.4 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。

操作步骤

- 使用以下命令查看 PIM 路由表：
  - **display pim 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 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

4.5 调整邻居控制参数

设备间通过交互 Hello 消息建立 PIM 邻居关系，协商各类控制参数，通过 Hello 消息中携带的控制参数来控制邻居关系。

4.5.1 建立配置任务

配置 PIM-DM 基本功能后，可以根据实际需要调整 Hello 消息的相关参数来控制邻居关系，配置邻居过滤功能来提高安全性。

应用环境

PIM 路由器之间通过交互 Hello 消息建立邻居关系，协商各类控制参数。

路由器在系统缺省值的控制下可以正常工作。同时，AR2200-S 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在调整邻居控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-DM 基本功能**

数据准备

在调整邻居控制参数之前，需准备以下数据。

序号	数据
1	邻居的超时时间
2	发送 Hello 消息的时间间隔
3	触发 Hello 消息的最大延迟
4	过滤 PIM 邻居的 ACL 号或 ACL 名字

4.5.2 配置发送 Hello 报文的时间间隔

发送 Hello 消息的时间间隔可以在全局和接口两种情况下配置。接口配置优于 PIM 视图下的配置，接口上未配置时 PIM 视图下的配置生效。

背景信息

在 PIM-DM 路由器上进行如下配置。

说明

PIM 邻居的控制参数可以在两种情况下配置：

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局性
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **timer hello** *interval*，配置发送 Hello 消息的时间间隔。
- 接口
  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 **pim timer hello** *interval*，配置发送 Hello 消息的时间间隔。

4. 执行命令 **pim triggered-hello-delay** *interval*，配置触发 Hello 消息的最大延迟，避免多个 PIM 路由器同时发送 Hello 消息而导致冲突。

----结束

4.5.3 配置邻居超时时间

邻居超时时间可以在全局和接口两种情况下配置。若超时设备仍没有收到 Hello 消息则认为邻居不可达。PIM 邻居超时时间应大于发送 Hello 消息的时间间隔。

背景信息

在 PIM-DM 路由器上进行如下配置。

说明

PIM 邻居的控制参数可以在两种情况下配置：

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局性
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **hello-option holdtime** *interval*，配置保持邻居为可达状态的超时时间，若超时仍没有收到 Hello 消息则认为邻居不可达。
- 接口
  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 **pim hello-option holdtime** *interval*，配置保持邻居为可达状态的超时时间，若超时仍没有收到 Hello 消息则认为邻居不可达。

----结束

4.5.4 拒绝接收无 Generation-ID 的 Hello 报文

当来自上游的 Hello 消息中的 Generation ID 发生改变，则表明上游邻居状态发生改变。可以配置 PIM 接口拒绝无 Generation ID 参数的 Hello 消息，从而实时了解上游邻居的状态。

背景信息

在 PIM-DM 路由器上进行如下配置。

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 require-genid**，配置 Hello 消息中应包含 Generation ID 选项，拒绝无 Generation ID 选项的 Hello 消息。

当来自上游的 Hello 消息中的 Generation ID 发生改变，则表明上游邻居状态发生改变（重启）。如果路由器不希望从上游收到数据，则在收到来自上游的数据报文后发送 Prune 消息。

----结束

4.5.5 配置邻居过滤

为了防止未知设备参与 PIM 协议，需要过滤 PIM 邻居。接口上只与符合过滤规则的地址建立邻居关系，删除不符合过滤规则的邻居。

背景信息

为了防止未知路由器参与 PIM 协议，需要过滤 PIM 邻居。

在运行 PIM-DM 的路由器上进行如下配置。

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* }，配置邻居过滤。

接口上只与符合过滤规则的地址建立邻居关系，删除不符合过滤规则的邻居。

说明

在接口上配置邻居过滤功能时，与该接口建立 PIM 邻居的路由器上都需要配置相应的邻居过滤功能。

----结束

4.5.6 检查配置结果

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

----结束

4.6 调整剪枝控制参数

当下游接口上最后一个组成员离开时，设备的上游接口发送 Prune 消息请求上游设备执行剪枝，同网段其他仍需要该组数据的下游设备必须发送 Join 消息来否决剪枝。

4.6.1 建立配置任务

配置 PIM-DM 基本功能后，可以根据实际需要配置接口保持剪枝状态的时间、LAN 内传输 Prune 消息的延迟时间和否决剪枝的时间间隔。

应用环境

当路由器上的最后一个组成员离开时，路由器从上游接口发出 Prune 消息，请求上游路由器执行剪枝操作，停止向该路由器转发组播数据。当该网段中还存在其他下游路由器时，其他下游路由器必须发送 Join 消息，否决剪枝操作。

路由器在系统缺省值的控制下可以正常的工作。同时，AR2200-S 允许用户根据具体环境，适当调整相关参数。

说明

剪枝的控制参数可以在两种情况下配置:

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

前置任务

在调整剪枝控制参数之前，需完成以下任务：

- 配置某单播路由协议
- 配置 PIM-DM（IPv6）基本功能

数据准备

在调整剪枝控制参数之前，需准备以下数据。

序号	数据
1	Prune 状态的超时时间
2	传递 Prune 剪枝消息的延迟时间
3	否决剪枝的时间

4.6.2 配置接口保持剪枝状态的时间

接口保持剪枝状态的超时时间可以在全局和接口两种情况下配置。超时后，被剪枝接口恢复转发。超时前收到状态刷新消息则重新计时。

背景信息

在 PIM-DM 路由器上进行如下配置。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **holdtime join-prune** *interval*，配置下游接口保持剪枝状态的时间。超时后，被剪枝接口恢复转发。超时前收到状态刷新消息则重新计时。
- 接口

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 **pim holdtime join-prune** *interval*，配置下游接口保持 Prune 状态的时间。超时后，被剪枝接口恢复转发。超时前收到状态刷新消息则重新计时。

----结束

4.6.3 配置 LAN 内传输 Prune 消息的延迟时间

LAN 内传输 Prune 消息的延迟时间可以在全局和接口两种情况下配置。当同一链路中的所有设备的 lan-delay 值不同时，将进行协商从中选取最大值。

背景信息

在 PIM-DM 路由器上进行如下配置。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **hello-option lan-delay** *interval*，配置在 LAN 内传输 Prune 消息的延迟时间。
- 接口
  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 **pim hello-option lan-delay** *interval*，配置在 LAN 内传输 Prune 消息的延迟时间。

----结束

4.6.4 配置否决剪枝的时间间隔

当同一网段中有设备向上游发送剪枝消息时，如果其他设备仍然需要接收组播数据，则必须在否决剪枝的时间内向上游发送 Join 消息。

背景信息

在 PIM-DM 路由器上进行如下配置。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **hello-option override-interval** *interval*，配置否决剪枝的时间。

     当同一网段中有路由器向上游发送剪枝消息时，如果其他路由器仍然需要接收组播数据，则必须在 override-interval 时间内向上游发送 Join 消息。
- 接口

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 **pim hello-option override-interval** *interval*，配置否决剪枝的时间。

----结束

4.6.5 检查配置结果

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

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

4.7 调整状态刷新控制参数

周期性的“扩散-剪枝”将造成很大的网络资源浪费。为防止被剪枝接口因为剪枝状态超时而恢复转发，系统启用了状态刷新功能，周期性的发送 State-Refresh 消息，刷新接口剪枝状态，维持 SPT 树。

4.7.1 建立配置任务

配置 PIM-DM 基本功能后，可以根据实际需要配置发送 State-Refresh 消息的时间间隔、接收下一个 State-Refresh 消息的时间和 State-Refresh 消息的 TTL 值。

应用环境

在 PIM-DM 网络中，周期性的扩散-剪枝将造成很大的网络资源浪费。为防止被剪枝接口因为状态超时而恢复转发，AR2200-S 允许用户启用状态刷新功能，周期性的发送 State-Refresh 消息，刷新接口剪枝状态，维持 SPT 树。

路由器在系统缺省值的控制下可以正常的工作。同时，AR2200-S 允许用户根据具体环境，适当调整相关参数。

说明

如果具体网络没有特殊要求，推荐采用缺省值。

前置任务

在调整状态刷新控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-DM 基本功能**

数据准备

在调整状态刷新控制参数之前，需准备以下数据。

序号	数据
1	发送 PIM 状态刷新消息的时间间隔
2	接收下个状态刷新消息前的等待时间
3	转发状态刷新消息的 TTL 值

4.7.2 禁止状态刷新功能

禁止该功能后，接口不转发 State-Refresh 消息。

背景信息

在 PIM-DM 域内所有路由器上进行如下配置。

说明

缺省情况下，接口启动 PIM-DM 状态刷新功能。

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 PIM-DM 状态刷新功能。禁止该功能的接口不转发状态刷新消息。

说明

使用命令 **pim state-refresh-capable** 可以重新启动接口上的 PIM-DM 状态刷新功能。

----结束

4.7.3 配置发送状态刷新消息的时间间隔

为了避免被剪枝接口因剪枝状态超时而恢复转发，状态刷新消息的发送间隔时间应小于保持剪枝状态的超时时间。

背景信息

在 PIM-DM 域内所有路由器上进行如下配置。

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** ，进入 PIM 视图。

步骤 3 执行命令 **state-refresh-interval** *interval*，配置发送 PIM 状态刷新消息的时间间隔。

说明

- 此命令适用于与组播源相连的第一跳路由器上。
- 状态刷新消息的发送间隔时间应该小于保持 Prune 状态的超时时间。
- 使用 **holdtime join-prune** 命令可以配置保持 Prune 状态的超时时间。

----结束

4.7.4 配置接收下一个状态刷新消息的时间

设备可能在很短的时间内收到来自多个设备的 State-Refresh 消息，而其中有些消息是重复的。状态刷新定时器超时前收到的重复消息被丢弃，超时后允许接收下一个 State-Refresh 消息。

背景信息

在 PIM-DM 域内所有路由器上进行如下配置。

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** ，进入 PIM 视图。

步骤 3 执行命令 **state-refresh-rate-limit** *interval*，配置接收下个状态刷新消息前的等待时间。

----结束

4.7.5 配置状态刷新消息的 TTL 值

设备在接收到 State-Refresh 消息后会将 TTL 值减 1，然后向下游转发，直到 TTL 值变为 0。当网络规模很小时，State-Refresh 消息将在网络中循环传递。可以根据网络规模大小配置合适的 TTL 值。

背景信息

在 PIM-DM 域内所有源直连的路由器上进行如下配置。

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** ，进入 PIM 视图。

步骤 3 执行命令 **state-refresh-ttl** *ttl-value*，配置转发状态刷新消息的 TTL 值。

说明

此命令只在源直连路由器上配置有效。

----结束

4.7.6 检查配置结果

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

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

为使网络中出现的新的组成员能够快速的接收到组播数据，设备会主动从上游接口发出 Graft 消息，请求上游设备向该网段转发组播数据。

4.8.1 建立配置任务

配置 PIM-DM 基本功能后，可以根据实际需要配置重传 Graft 消息的时间间隔。

应用环境

在 PIM-DM 网络中，如果未启用状态刷新功能，被剪枝接口必须等到状态超时后才会恢复转发。如果启用了状态刷新功能，则有可能永远也不会恢复转发。

为使网络中出现的新的组成员能够快速的接收到组播数据，PIM-DM 路由器会主动从上游接口发出 Graft 消息，请求上游路由器向该网段转发组播数据。上游路由器收到 Graft 消息后，立即回复 Graft-Ack 消息，并将收到该 Graft 消息的接口恢复转发。

路由器在系统缺省值的控制下可以正常的工作。同时，AR2200-S 允许用户根据具体环境，适当调整相关参数。

说明

如果具体网络没有特殊要求，推荐采用缺省值。

前置任务

在调整嫁接控制参数之前，需完成以下任务：

- 配置某单播路由协议
- 配置 PIM-DM 基本功能

数据准备

在调整嫁接控制参数之前，需准备以下数据。

序号	数据
1	重传 Graft 嫁接消息的时间间隔

4.8.2 配置重传 Graft 嫁接消息的时间间隔

当有成员加入曾经被剪枝的组时，设备发出 Graft 消息，并等待上游确认。如果在一定时间内没有收到确认消息，设备将重传嫁接消息，直到收到上游的确认消息。

背景信息

在 PIM-DM 路由器上进行如下配置。

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*，配置重传 Graft 嫁接消息的时间间隔。

当路由器在指定时间内都没有接收到来自上游的 Graft-Ack 嫁接确认消息，则会重发 Graft 嫁接消息，以期待嫁接操作得到上游路由器的确认。

----结束

4.8.3 检查配置结果

调整嫁接控制参数成功后，可以通过命令查看未确认的 PIM-DM 嫁接信息、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 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看接口上的 PIM 信息。
- 使用 **display pim grafts** 命令查看未确认的 PIM-DM 嫁接信息。

- 使用 **display pim control-message counters** [**message-type** { **assert** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** | **bsr** } | **interface** *interface-type interface-number*] * 命令查看发送和接收 PIM 控制报文的数目信息。
- 使用以下命令查看 PIM 路由表：
  - **display pim 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 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

4.9 调整 Assert 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 消息，参与竞选唯一上游。

4.9.1 建立配置任务

配置 PIM-DM 基本功能后，可以根据实际需要配置保持 Assert 状态的时间。

应用环境

当 PIM-DM 路由器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路由器。路由器从该接口发出 Assert 消息，参与竞选唯一上游。

路由器在系统缺省值的控制下可以正常的工作。同时，AR2200-S 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在调整 Assert 控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-DM 基本功能**

数据准备

在调整 Assert 控制参数之前，需准备以下数据。

序号	数据
1	保持 Assert 状态的时间

4.9.2 配置保持 Assert 状态的时间

落选设备保持 Assert 状态的时间内禁止下游接口转发组播数据，超时后恢复转发。

背景信息

在 PIM-DM 路由器上进行如下配置。

说明

Assert 控制参数可以在两种情况下配置：

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **holdtime assert** *interval*，配置保持 Assert 状态的时间。落选路由器在此时间内禁止下游接口转发组播数据，超时后恢复转发。
- 接口
  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 **pim holdtime assert** *interval*，配置保持 Assert 状态的时间。落选路由器在此时间内禁止下游接口转发组播数据，超时后恢复转发。

----结束

4.9.3 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 控制消息统计数和 PIM 路由表等信息。

操作步骤

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

4.10 配置防止主机恶意攻击功能（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。

4.10.1 建立配置任务

网络中 PIM-DM 和 IGMP 的基本功能都已配置后，将 PIM Silent 特性配置在与主机相连的接口上，该接口使能了 PIM-DM 和 IGMP。

应用环境

在接入层上，路由器直连用户主机的接口上需要使能 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 PIM Hello 报文，大量发送时，有可能导致路由器瘫痪。

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。同时，该接口上的 IGMP 功能不受影响。

该功能的使用环境是：

- 仅适用于与用户主机网段直连的路由器接口，且该用户网段只与这一台路由器相连。

注意

如果在与路由器相连的接口上启动该功能，将导致 PIM 邻居无法正常建立，引发组播故障。如果用户网段与多台路由器相连，在多个路由器接口上配置 PIM Silent，则这些接口都不会发送 Assert 消息，导致该网段存在多个组播数据转发接口，从而引发组播故障。

前置任务

在配置防止主机恶意攻击功能之前，需要完成以下任务：

- 配置单播路由协议，使网络畅通
- 配置 PIM-DM
- 配置 IGMP

数据准备

在配置防止主机恶意攻击功能之前，需要准备以下数据。

序号	数据
1	与用户主机相连的路由器接口类型和编号

4.10.2 配置 PIM Silent

配置 PIM Silent 后，接口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，并自动成为 DR。同时，该接口上的 IGMP 功能不受影响。

背景信息

在连接主机网段的接口上进行如下配置。

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。可以有效的防范恶意主机 Hello 报文攻击，保护路由器。

----结束

4.10.3 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。

前提条件

已经完成防止主机恶意攻击功能（PIM Silent）功能的所有配置。

操作步骤

步骤 1 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看 PIM 接口信息。

----结束

任务示例

执行命令 **display pim interface verbose**，可以看到使能了此配置。

```
<Huawei> display pim interface gigabitethernet 1/0/0 verbose
 VPN-Instance: public net
 Interface: GigabitEthernet1/0/0, 10.1.2.1
     PIM version: 2
     PIM mode: Sparse
     PIM state: up
     PIM DR: 10.1.2.2 (local)
     PIM DR Priority (configured): 1
     PIM neighbor count: 0
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM hello override interval (negotiated): 2500 ms
```

```
PIM hello override interval (configured): 2500 ms
PIM Silent: enabled
PIM neighbor tracking (negotiated): disabled
PIM neighbor tracking (configured): disabled
PIM generation ID: 0X4B9F5B92
PIM require-GenID: disabled
PIM hello hold interval: 105 s
PIM assert hold interval: 180 s
PIM triggered hello delay: 5 s
PIM J/P interval: 60 s
PIM J/P hold interval: 210 s
PIM BSR domain border: disabled
PIM BFD: disabled
PIM dr-switch-delay timer : not configured
Number of routers on link not using DR priority: 0
Number of routers on link not using LAN delay: 0
Number of routers on link not using neighbor tracking: 1
ACL of PIM neighbor policy: -
ACL of PIM ASM join policy: -
ACL of PIM SSM join policy: -
ACL of PIM join policy: -
```

4.11 维护 PIM-DM（IPv4）

PIM-DM 的维护包括：清除 PIM 统计信息。

4.11.1 清除 PIM 控制报文统计信息

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。

背景信息

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

步骤 1 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 control-message counters** [**interface** *interface-type interface-number*]命令。

----结束

4.12 配置举例

通过配置举例，可以了解如何构建基本的 PIM-DM 网络。

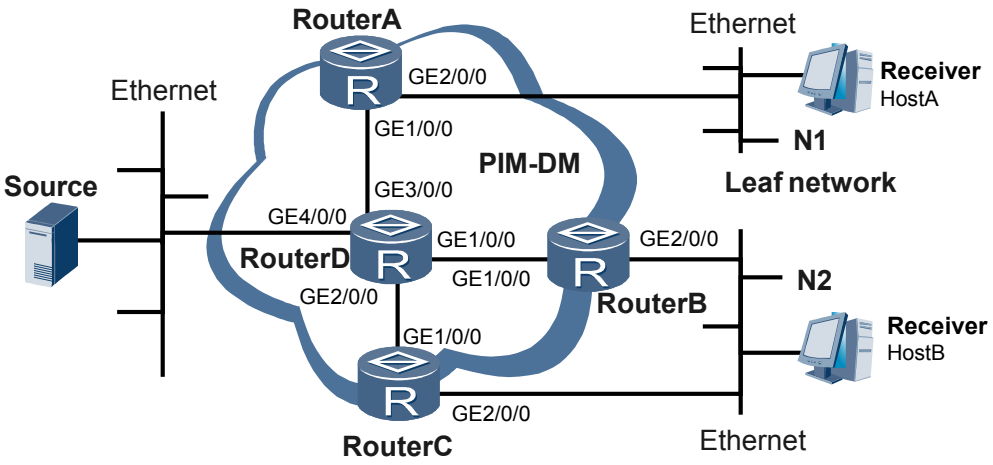
4.12.1 配置 PIM-DM 基本功能组网示例

在单播路由正常的 AS 内配置 PIM-DM 基本功能，使用户能够接收任意组播源发送的数据。

组网需求

在如图 4-2 所示的试验网中部署组播功能。已知网络中已经部署了完备的 IGP，单播运行正常。要求通过在路由器上进行适当配置，使网络中的用户主机能够通过组播方式接收视频信息。

图 4-2 配置 PIM-DM 基本功能组网图



Device	接口	IP 地址	Device	接口	IP 地址
Router A	GE 1/0/0	192.168.1.1/24	Router D	GE 1/0/0	192.168.2.2/24
	GE 2/0/0	10.110.1.1/24		GE 2/0/0	192.168.3.2/24
Router B	GE 1/0/0	192.168.2.1/24		GE 3/0/0	192.168.1.2/24
	GE 2/0/0	10.110.2.1/24		GE 4/0/0	10.110.5.1/24
Router C	GE 1/0/0	192.168.3.1/24			
	GE 2/0/0	10.110.2.2/24			

配置思路

由于网络环境是规模较小的试验网，采用 PIM-DM 协议配置组播功能。在 RouterA 上使能 PIM Silent，防范 Hello 报文攻击。

1. 在路由器上使能组播功能。
2. 在接口上使能 PIM-DM 功能。
3. 在与主机相连的接口上使能 PIM Silent，配置 IGMP。

数据准备

为完成此配置举例，需准备如下的数据：

- 组播组 G 地址：225.1.1.1/24。
- 组播源 S 地址：10.110.5.100/24。
- 路由器和用户主机之间运行的 IGMP 版本号为 2。

操作步骤

步骤 1 配置各 Router 接口 IP 地址和单播路由协议。

按照图 4-2 配置各接口的 IP 地址和掩码，并配置各 Router 之间采用 OSPF 进行互连，确保网络中各 Router 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。具体配置过程略，详见配置文件。

步骤 2 使能组播功能，并在各接口上使能 PIM-DM 功能

在 RouterA 上使能组播功能，在各接口上使能 PIM-DM 功能。RouterB、RouterC 和 RouterD 上的配置过程与 RouterA 上的配置相似，配置过程略，详见配置文件。

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

步骤 3 在与主机相连的接口上使能 PIM Silent，配置 IGMP

在 RouterA 连接用户主机的接口上使能 PIM Silent，配置 IGMP 功能。

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

在 RouterB 连接用户主机的接口上配置 IGMP。RouterC 上的配置过程与 RouterB 上的配置相似，配置过程略，详见配置文件。

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

步骤 4 检验配置效果

通过使用 **display pim interface** 命令可以查看路由器接口上 PIM 的配置和运行情况。例如 RouterD 上 PIM 配置的显示信息如下：

```
<RouterD> display pim interface
VPN-Instance: public net
Interface      State   NbrCnt   HelloInt   DR-Pri     DR-Address
GE1/0/0        up      1        30         1          192.168.2.2    (local)
GE2/0/0        up      1        30         1          192.168.3.2    (local)
GE3/0/0        up      1        30         1          192.168.1.2    (local)
GE4/0/0        up      0        30         1          10.110.5.1     (local)
```

通过使用 **display pim neighbor** 命令可以查看路由器之间的 PIM 邻居关系。例如 RouterD 上 PIM 邻居关系的显示信息如下：

```
<RouterD> display pim neighbor
VPN-Instance: public net
 Total Number of Neighbors = 3
 Neighbor        Interface         Uptime       Expires      Dr-Priority
 192.168.1.1     GE3/0/0           00:02:22     00:01:27     1
 192.168.2.1     GE1/0/0           00:00:22     00:01:29     1
 192.168.3.1     GE2/0/0           00:00:23     00:01:31     1
```

通过使用 **display pim routing-table** 命令可以查看路由器 PIM 协议组播路由表。假如 HostA 需要接收组播组 G（225.1.1.1/24）的信息。当组播源 S（10.110.5.100/24）向组播组 G 传送组播报文时，通过扩散生成组播分发树，组播分发树路径中各路由器（RouterA 和 RouterD）上都存在（S，G）表项，HostA 加入组播组 G，在 RouterA 上生成（*，G）表项，RouterB 和 RouterC 上的显示信息和 RouterA 类似。显示信息如下：

```
<RouterA> display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry
 (*, 225.1.1.1)
     Protocol: pim-dm, Flag: WC
     UpTime: 03:54:19
     Upstream interface: NULL
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/0
             Protocol: igmp, UpTime: 01:38:19, Expires: never
(10.110.5.100, 225.1.1.1)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:00:44
     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: GigabitEthernet2/0/0
              Protocol: pim-dm, UpTime: 00:00:44, Expires: never
<RouterD> display pim routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry
 (10.110.5.100, 225.1.1.1)
     Protocol: pim-dm, Flag: LOC ACT
     UpTime: 01:35:25
     Upstream interface: GigabitEthernet4/0/0
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 3
        1: GigabitEthernet3/0/0
            Protocol: pim-dm, UpTime: 00:03:27, Expires: never
        2: GigabitEthernet1/0/0
            Protocol: pim-dm, UpTime: 00:03:27, Expires: never
        3: GigabitEthernet2/0/0
            Protocol: pim-dm, UpTime: 00:03:27, Expires: never
```

----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 dm
#
interface GigabitEthernet2/0/0
 ip address 10.110.1.1 255.255.255.0
 pim dm
 pim silent
 igmp enable
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 10.110.1.0 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 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 192.168.2.0 0.0.0.255
  network 10.110.2.0 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 dm
#
interface GigabitEthernet2/0/0
 ip address 10.110.2.2 255.255.255.0
 pim dm
 igmp enable
#
ospf 1
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 10.110.2.0 0.0.0.255
#
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 dm
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.2 255.255.255.0
 pim dm
#
interface GigabitEthernet3/0/0
 ip address 192.168.1.2 255.255.255.0
 pim dm
#
interface GigabitEthernet4/0/0
 ip address 10.110.5.1 255.255.255.0
 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 192.168.1.0 0.0.0.255
  network 10.110.5.0 0.0.0.255
#
return
```

5 PIM-SM（IPv4）配置

关于本章

通过配置 PIM 协议，可以实现 AS 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。

5.1 PIM-SM 概述
在组成员分布非常稀疏，几乎所有网段均不存在组成员的网络中，RP 是 PIM-SM 网络的转发核心，网络中所有 PIM 设备都知道 RP 的位置，组成员和组播源的信息都向 RP 汇聚。

5.2 AR2200-S 支持的 PIM-SM 特性
系统允许用户根据具体环境适当调整邻居、转发、DR、RP、加入、注册和 Assert 等相关参数，通过配置各种过滤策略和 PIM Silent 功能来提高 PIM-SM 的安全性。PIM-SM 网络支持 SSM、PIM BFD。

5.3 配置 PIM-SM 基本功能
在单播路由畅通的情况下，在每台设备上使能 IPv4 组播路由，在设备的每个接口上使能 PIM-SM，在网络中配置静态 RP 或动态 RP，PIM-SM 网络就可以正常运行了。

5.4 调整组播源控制参数
设备可以基于组播源来控制组播报文的转发。一方面有助于数据流量控制，另一方面可以限定下游接收者能够获得的信息，提高安全性。

5.5 调整 C-RP 和 C-BSR 的控制参数
使用动态 RP 时，可以根据实际网络情况调整 C-RP 和 C-BSR 的各项参数。如无特殊要求，推荐使用缺省值。

5.6 配置 BSR 管理域
将 PIM-SM 网络划分为多个 BSR 管理域和一个 Global 域，可以分担单一 BSR 的管理压力，还可以使用私有组地址为特定区域的用户提供专门服务。

5.7 调整邻居控制参数
设备间通过交互 Hello 消息建立 PIM 邻居关系，协商各类控制参数。可以根据实际需要调整 Hello 消息中携带的参数，若无特殊要求推荐采用缺省值。

5.8 调整源注册控制参数

与组播源直连的 DR 将接收到的组播数据逐一封装到 Register 消息中，以单播方式发送到 RP。RP 将解封装后的组播数据沿 RPT 转发到接收者。系统允许配置 Register 消息过滤和注册抑制功能。

5.9 调整转发控制参数

设备向上游发送 Join 消息请求转发组播数据，发送 Prune 消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。

5.10 调整 Assert 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 消息，参与竞选唯一上游。

5.11 配置基于 PIM 协议的 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。

5.12 配置防止主机恶意攻击功能（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。

5.13 维护 PIM-SM（IPv4）

PIM-SM 的维护包括：清除 PIM 统计信息。

5.14 配置举例

通过配置举例，可以了解如何构建基本的 PIM-SM 网络、配置 PIM-SM 常用功能。

5.1 PIM-SM 概述

在组成员分布非常稀疏，几乎所有网段均不存在组成员的网络中，RP 是 PIM-SM 网络的转发核心，网络中所有 PIM 设备都知道 RP 的位置，组成员和组播源的信息都向 RP 汇聚。

PIM（Protocol Independent Multicast）称为协议无关组播，表示为 IP 组播提供路由信息的可以是静态路由、RIP、OSPF、IS-IS、BGP 等任何单播路由协议。组播路由和单播路由协议无关，只是通过单播路由表产生相应组播路由表项。

PIM 借助 RPF（Reverse Path Forwarding）机制实现组播报文转发。RPF 机制利用现存的单播路由信息在网络中构建组播转发树。当一个组播报文到达路由器时，首先进行 RPF 检查。RPF 检查通过，则创建相应组播路由表项，从而进行组播报文转发。RPF 检查失败，则将该报文丢弃。

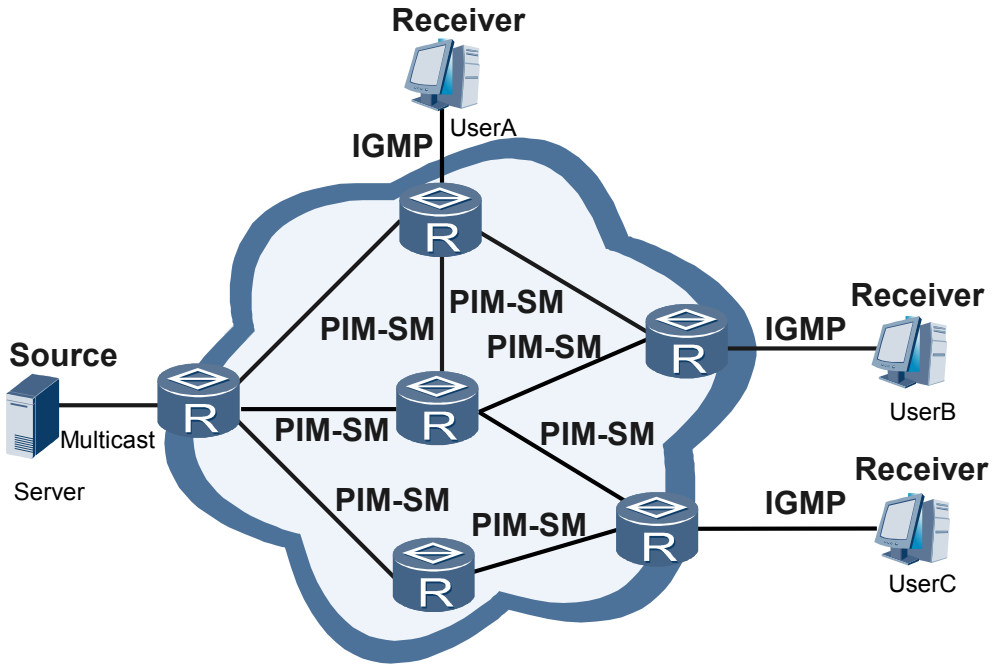
说明

关于 RPF 的详细说明请参见《Huawei AR2200-S 系列 **IPv4 组播路由管理**》。

PIM-SM（Protocol Independent Multicast-Sparse Mode）称为协议无关组播－稀疏模式，属于稀疏模式的组播路由协议。PIM-SM 的工作过程主要有：邻居发现、Assert、DR 选举、RP 发现、加入、剪枝、注册、SPT 切换。

如图 5-1 所示，PIM-SM 适用于组成员分布相对分散、范围较广、大规模的网络。

图 5-1 PIM-SM 在组播网络中的应用



说明

- 对于组成员分布相对密集的小型网络适用 PIM-DM（Protocol Independent Multicast Dense Mode）。
- 使用 PIM-SM 协议，可以构建 ASM（Any-Source Multicast）和 SSM（Source-Specific Multicast）两种组播模型。

5.2 AR2200-S 支持的 PIM-SM 特性

系统允许用户根据具体环境适当调整邻居、转发、DR、RP、加入、注册和 Assert 等相关参数，通过配置各种过滤策略和 PIM Silent 功能来提高 PIM-SM 的安全性。PIM-SM 网络支持 SSM、PIM BFD。

说明

异步串口，ISDN BRI 接口，3G 接口，Bridge-if 接口，NULL 接口，QinQ 子接口不支持 PIM-SM。

PIM-SM 基本功能

PIM-SM 支持 ASM 和 SSM 两种组播模型，用户可以根据需要配置 ASM 或 SSM 组地址的范围。

静态 RP

用户可以在 PIM-SM 域的所有路由器上指定静态 RP。当域内存在动态 RP 时，缺省的是动态 RP 优先，但用户可以通过配置来优先使用静态 RP。

动态 RP

用户可以在 PIM-SM 域内配置 C-RP 和 C-BSR，经过统一的规则动态产生 BSR 和 RP。用户可以调整 C-RP 的竞选优先级、调整 C-RP 发送的 Advertisement 宣告消息在 BSR 上的存活时间、调整 C-RP 发送 Advertisement 宣告消息的时间间隔和通过指定 ACL 来限制 C-RP 服务的组播组范围。

BSR

用户可以在 BSR 域内指定 C-BSR，并且可以调整用于 C-RP 竞选 RP 的哈希掩码长度、调整用于竞选 BSR 的优先级，以及合法的 BSR 的地址范围。同时还可以在 BSR 域边界的路由器接口上配置 BSR 服务边界，以限制 BSR 消息的传播。

控制组播源

用户可以通过配置组播源地址过滤规则来控制组播源。还可以通过策略过滤 Register 报文，抑制 PIM-SM 注册消息。

BSR 管理域

用户可以配置 BSR 管理域的服务边界和管理域边界。

调整 PIM-SM 邻居参数

用户可以调整 PIM-SM 邻居之间的控制参数，包括：

- 发送 Hello 报文的时间间隔。
- 保持邻居状态为可达的超时时间。
- 是否接收包含 Generation ID 的 Hello 消息。
- 触发 Hello 消息的最大延迟时间。
- 竞选 DR 的优先级。
- DR 切换延迟时间。
- 邻居过滤功能。接口上只与符合过滤规则的地址建立邻居关系。

调整转发控制参数

用户可以调整转发控制参数，包括：

- 发送 Join 消息的时间间隔。
- 下游接口保持转发状态的时间。
- 否决剪枝的时间。
- 过滤 Join/Prune 消息中的 Join 信息。
- 邻居检查功能。接收或发送 Join/Prune 消息和 Assert 消息时，检查该消息是否来自 PIM 邻居或发送给 PIM 邻居，如果不是则不处理。

调整 Assert 控制参数

用户可以配置路由器接口保持 Assert 状态的时间。

PIM BFD

AR2200-S 支持 PIM 邻居之间动态创建 BFD 会话检测邻居之间的链路状态，一旦有故障，BFD 会把结果直接通告给 PIM。

PIM Silent

在接入层上，路由器连接用户主机的接口上需要使能 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 PIM hello 报文，大量发送时，有可能导致路由器瘫痪。

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。

PIM for Anycast RP

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。

5.3 配置 PIM-SM 基本功能

在单播路由畅通的情况下，在每台设备上使能 IPv4 组播路由，在设备的每个接口上使能 PIM-SM，在网络中配置静态 RP 或动态 RP，PIM-SM 网络就可以正常运行了。

5.3.1 建立配置任务

在配置 PIM-SM 基本功能之前，需配置 IPv4 单播路由协议。

应用环境

一个 PIM-SM 网络可以同时采用 ASM 与 SSM 模型为用户主机提供组播服务。首先必须在网络中配置完备的 ASM 模型部件，包括 RP，然后根据实际需要调整 SSM 组地址范围。

说明

SSM 模型需要 IGMPv3 版本的支持。如果用户主机必须运行 IGMPv1 或 v2，则需要在路由器接口上配置 IGMP SSM Mapping。

路由器通过 IGMP 得知用户希望加入的组播组 G。

- 如果 G 在 SSM 组地址范围内，且用户通过 IGMPv3 加入组 G 时明确指定了 S。则采用 SSM 模型提供组播服务。
- 如果 G 在 SSM 组地址范围内，且路由器上静态配置了（S，G）SSM Mapping 规则。则采用 SSM 模型提供组播服务。
- 如果 G 在 SSM 组地址范围外，则采用 ASM 模型提供组播服务。

PIM-SM 中的 ASM 模型支持两种获得 RP 的方法，用户根据需要选择配置即可：

- 动态 RP：需要在 PIM-SM 域内选取几台路由器，配置 C-RP 和 C-BSR；在域边界路由器接口上配置 BSR 边界。PIM-SM 域内的每一台路由器会自动获得 RP。
- 静态 RP：必须在 PIM-SM 域内的每一台路由器上手动配置 RP。对于大型 PIM 网络，配置静态 RP 将会非常繁琐。所以，通常只将静态 RP 作为动态 RP 的备份，用来提高网络的健壮性，增强组播网络的运营管理能力。

一个组播组可能同时属于动态 RP 和静态 RP 的服务范围。缺省情况下，路由器优先选取动态 RP，如果配置了静态 RP 优先，则优先选用静态 RP。

不同的组播组对应不同的 RP，与所有组播组对应同一个 RP 相比，可以减轻单个 RP 的负荷，增强网络的健壮性。

前置任务

在配置 PIM-SM 基本功能之前，需完成以下任务：

- 配置单播路由协议

数据准备

在配置 PIM-SM 基本功能之前，需准备以下数据。

序号	数据
1	静态 RP 地址
2	定义了静态 RP 所服务的组播组范围的 ACL
3	C-RP 的优先级
4	定义了 C-RP 所服务的组播组范围的 ACL

序号	数据
5	C-RP 发送 Advertisement 宣告消息的间隔时间
6	BSR 等待接收 C-RP 发送的 Advertisement 宣告消息的超时时间
7	C-BSR 的哈希掩码长度
8	C-BSR 的优先级
9	SSM 组地址范围

5.3.2 使能 IP 组播路由

使能 IPv4 组播路由是配置所有 IPv4 组播特性的首要步骤。

背景信息

在路由器上进行如下配置。

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 **multicast routing-enable**，使能公网实例 IP 组播路由。

----结束

5.3.3 使能 PIM-SM 功能

接口上使能了 PIM-SM 后，才可以和其他设备建立 PIM 邻居。

背景信息

说明

同一接口上不能同时使能 PIM-DM 和 PIM-SM 功能，而且路由器上属于同一实例的所有接口的 PIM 模式必须相同。当路由器被部署在 PIM-SM 域中时，建议在全部非边界接口上使能 PIM-SM 功能。

在路由器上进行如下配置。

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 sm**，使能 PIM-SM 功能。在接口上使能了 PIM-SM 功能后，路由器之间建立 PIM 邻居，从而才能对来自 PIM 邻居的协议报文进行处理。

----结束

5.3.4 （可选）配置静态 RP

当网络内仅有一个 RP 时，可以手工配置静态 RP，这样可以避免 C-RP 和 BSR 之间频繁的信息交互占用带宽。PIM-SM 域内所有设备都必须配置完全相同的静态 RP。

背景信息

注意

在 PIM-SM 网络中同时配置静态 RP 和动态 RP，容易引发网络故障，请慎重选择是否进行此项配置。若希望在 PIM-SM 网络中仅使用动态 RP，则跳过此项配置。

在 PIM-SM 域中所有路由器上进行如下配置。未配置静态 RP 的路由器不能参与此 PIM-SM 域内的组播转发。

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** ，进入 PIM 视图。

步骤 3 执行命令 **static-rp** *rp-address* [*basic-acl-number* | **acl-name** *acl-name*] [**preferred**]，指定静态 RP。重复执行该命令可以为路由器配置多个静态 RP。

说明

PIM-SM 域内所有路由器都必须配置完全相同的 **static-rp** 命令。

- *rp-address* 为静态 RP 地址。
- *basic-acl-number* | **acl-name** *acl-name* 为访问控制列表，该列表定义了静态 RP 所服务的组播组范围。当多个静态 RP 服务的组播组范围有重叠时，IP 地址最大的静态 RP 成为真正为组播组提供服务的 RP。
- **preferred** 表示静态 RP 优先。如果网络中同时还配置了 C-RP，配置 **preferred** 后，路由器优先选用静态指定的 RP。否则优先选取 C-RP。

----结束

5.3.5 （可选）配置动态 RP

在 PIM-SM 域内选择几台 PIM 设备配置 C-RP，从 C-RP 中竞选产生 RP。必须同时配置 C-BSR，由 C-BSR 竞选产生 BSR，BSR 负责收集并发布网络中的 C-RP 信息。系统支持 Auto-RP 监听功能。

背景信息

注意

此项配置只适用于动态 RP，若希望网络中仅使用静态 RP，请跳过此项配置。

在 PIM-SM 域中有待成为 RP 的路由器上进行如下配置。

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** ，进入 PIM 视图。

步骤 3 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*] *，配置 C-RP。

- *interface-type interface-number* 为 C-RP 所在接口，该接口必须使能 PIM-SM。
- **group-policy** { *basic-acl-number* | **acl-name** *acl-name* }指定 C-RP 服务范围为 ACL 允许的组播组。缺省情况下，C-RP 为所有组播组服务。
- **priority** *priority* 为 C-RP 的竞选优先级，数值越大，优先级越低。缺省值是 0。

  在 RP 选举中，优先级较高的 C-RP 较优；优先级相同的情况下，执行 Hash 函数，计算结果较大者获胜；如果 Hash 函数计算结果也相同，比较 IP 地址，IP 地址较高者较优。

  说明

  推荐将 Loopback 接口配置为 RP。

  如果配置了接口地址借用，不建议将地址相同的接口同时配置为 C-RP。因为若优先级不相同，BSR 会认为 C-RP 的配置在不停的被修改。
- **holdtime** *hold-interval* 为 BSR 等待接收 C-RP 发送的 Advertisement 宣告消息的超时时间。缺省值是 150 秒。
- **advertisement-interval** *adv-interval* 为 C-RP 发送 Advertisement 宣告消息的时间间隔。缺省值是 60 秒。

步骤 4 执行命令 **c-bsr** *interface-type interface-number* [*hash-length* [*priority*]]，配置 C-BSR。

- *interface-type interface-number* 为 C-BSR 所在接口，该接口必须使能 PIM-SM。
- *hash-length* 为哈希掩码长度。路由器根据组地址 G、C-RP 的地址和 *hash-length*，运用 Hash 函数，对希望为组 G 服务且优先级相同的 C-RP 逐一进行计算，并比较计算结果。计算结果最大者成为真正为组 G 提供服务的 RP。
- *priority* 为候选优先级，数值越大，优先级越高。缺省值是 0。

  在 BSR 选举中，优先级较大者较优；优先级相同的情况下，IP 地址较高者较优。

步骤 5 （可选）执行命令 **bsm semantic fragmentation**，使能 BSR 报文分片功能。

推荐网络中所有设备都使能 BSR 报文分片功能，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。

步骤 6 （可选）执行命令 **auto-rp listening enable**，使能 Auto-RP 监听功能。

当路由器与支持 Auto-RP 的设备互通时，需要配置此命令。

----结束

5.3.6 （可选）配置 SSM 组播组地址范围

SSM 的组地址缺省范围是 232.0.0.0/8，可以手工配置 SSM 组播组地址范围，需要确保网络内所有设备配置的 SSM 组地址范围都一致。

背景信息

在 PIM-SM 网络中的所有路由器上进行如下配置。此项配置可选，缺省范围是 232.0.0.0/8。

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** ，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

确保网络内所有路由器上配置的 SSM 组地址范围都一致。

----结束

5.3.7 检查配置结果

配置 PIM-SM 基本功能成功后，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 **display pim bsr-info** 命令查看 PIM-SM 域中 BSR 自举路由器的信息。
- 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看接口上的 PIM 信息。
- 使用 **display pim neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *命令查看 PIM 邻居信息。
- 使用以下命令查看 PIM 路由表：
  - **display pim 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 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 **display pim rp-info** [*group-address*]命令查看 PIM-SM 域中的 RP 信息。

----结束

5.4 调整组播源控制参数

设备可以基于组播源来控制组播报文的转发。一方面有助于数据流量控制，另一方面可以限定下游接收者能够获得的信息，提高安全性。

5.4.1 建立配置任务

配置 PIM-SM 基本功能后，可以根据实际需要配置源生存时间和源地址过滤规则。

应用环境

本节所有配置同时适用于 ASM 模型和 SSM 模型。

PIM 路由器对流经自己的组播数据进行检查，通过比较是否符合过滤规则，判断组播报文是否继续转发。这时，可以将路由器看作组播数据的过滤器。过滤器的存在一方面有助于实现数据流量控制，另一方面可以在安全性方面限定下游接收者能够获得的信息。

路由器在系统缺省值的控制下可以正常地工作。同时，AR2200-S 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在控制组播源转发之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-SM 基本功能**

数据准备

在控制组播源转发之前，需准备以下数据。

序号	数据
1	组播源生存时间
2	组播源地址过滤规则

5.4.2 配置源生存时间

设备为每个(S,G)表项建立一个定时器。如果设备在“源生存时间”内没有收到 S 发出的组播报文，则认为(S,G)表项失效，组播源停止向组 G 发送组播数据。

背景信息

在 PIM 路由器上进行如下配置。

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** ，进入 PIM 视图。

步骤 3 执行命令 **source-lifetime** *interval*，配置组播源生存时间，超时则（S，G）表项失效。

----结束

5.4.3 配置源地址过滤

通过配置 ACL 规则，设备会根据源地址或源/组地址过滤接收的组播报文。

背景信息

在 PIM 路由器上进行如下配置。

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** ，进入 PIM 视图。

步骤 3 执行命令 **source-policy** { *acl-number* | **acl-name** *acl-name* }，配置过滤器。

如果配置的是基本 ACL，则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，则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。

说明

- 如果配置 *acl-number* | **acl-name** *acl-name* 的过滤规则，采用 **source-policy** 命令可以转发源地址或源地址及组地址属于过滤规则允许范围的组播报文。
- 如果仅指定 *acl-number* | **acl-name** *acl-name*，不配置其过滤规则，采用 **source-policy** 命令不转发任何源地址发送的组播报文。
- **source-policy** 命令不过滤静态（S，G）和记录了私网加入信息的 PIM 表项。

----结束

5.4.4 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。

操作步骤

- 使用以下命令查看 PIM 路由表：
  - **display pim 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 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

5.5 调整 C-RP 和 C-BSR 的控制参数

使用动态 RP 时，可以根据实际网络情况调整 C-RP 和 C-BSR 的各项参数。如无特殊要求，推荐使用缺省值。

5.5.1 建立配置任务

使用动态 RP 配置 PIM-SM 基本功能后，可以根据实际需要调整 C-RP 和 C-BSR 的参数、配置 BSR 服务边界和合法 BSR、C-RP 的地址范围。

应用环境

本节介绍在 ASM 模型中如何通过命令调整 C-RP 和 C-BSR 的控制参数。

说明

此项配置仅适用于 BSR-RP，若希望 PIM-SM 网络中仅使用静态 RP，请跳过本节。

路由器在系统缺省值的控制下可以正常的工作。同时，AR2200-S 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在调整 C-RP 和 C-BSR 的控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-SM 基本功能**

数据准备

在调整 C-RP 和 C-BSR 的各项参数之前，需准备以下数据。

序号	数据
1	C-RP 的优先级
2	C-RP 发送 Advertisement 宣告消息的间隔时间
3	BSR 等待接收 C-RP 发送的 Advertisement 宣告消息的超时时间
4	C-BSR 的哈希掩码长度
5	C-BSR 的优先级
6	C-BSR 发送 Bootstrap 自举消息的间隔时间
7	保持来自 BSR 的 Bootstrap 自举消息的时间
8	定义了合法 BSR 和 C-RP 的地址范围的 ACL

5.5.2 调整 C-RP 参数

C-RP 向 BSR 周期性发送 Advertisement 消息，Advertisement 消息中携带 C-RP 优先级等信息。可以在配置了 C-RP 的设备上调整 C-RP 优先级、发送 Advertisement 消息的周期、Advertisement 消息的有效时间。

背景信息

在已经配置了 C-RP 的路由器上进行如下配置。

说明

此项配置可以重新设置 C-RP 的各项参数。此项配置可选。如果没有特殊要求，推荐使用缺省值。

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** ，进入 PIM 视图。

步骤 3 执行命令 **c-rp priority** *priority*，配置 C-RP 优先级。

步骤 4 执行命令 **c-rp advertisement-interval** *interval*，配置 C-RP 发送 Advertisement 宣告消息的间隔时间。

步骤 5 执行命令 **c-rp holdtime** *interval*，配置保持来自 C-RP 的 Advertisement 宣告消息的时间。该参数值必须大于“C-RP 发送 Advertisement 宣告消息的间隔时间”。

C-RP 向竞选获胜的 BSR 周期性地发送 Advertisement 宣告消息。BSR 接收到这些宣告消息后，从中会读出 C-RP 的保持时间，即在此时间段内 C-RP 有效，超过该时间段，此 C-RP 老化。

----结束

5.5.3 调整 C-BSR 参数

最初，每个 C-BSR 都认为自己是 BSR，向所有设备发送 Bootstrap 消息。可以在配置了 C-BSR 的设备上调整 Bootstrap 消息中携带的 C-BSR 哈希掩码长度、C-BSR 优先级、发送 Bootstrap 消息的周期、Bootstrap 消息的有效时间。

背景信息

在已经配置了 C-BSR 的路由器上进行如下配置。

说明

此项配置可以重新设置 C-BSR 的各项参数。此项配置可选，如果没有特殊要求，推荐使用缺省值。

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** ，进入 PIM 视图。

步骤 3 执行命令 **c-bsr hash-length** *hash-length*，配置 C-BSR 的哈希掩码长度。

步骤 4 执行命令 **c-bsr priority** *priority*，配置 C-BSR 的优先级。

步骤 5 执行命令 **c-bsr interval** *interval*，配置 BSR 发送 Bootstrap 自举消息的间隔时间。

步骤 6 执行命令 **c-bsr holdtime** *interval*，配置保持来自 BSR 的 Bootstrap 自举消息时间。

BSR 周期性地向网络发送自举消息，接收到该消息的路由器会将自举消息保持一段时间，在该时间内 BSR 选举过程暂停；如果保持时间超时，则 C-BSR 之间会触发新一轮 BSR 选举过程。

说明

确保“保持来自 BSR 的 Bootstrap 自举消息时间”大于“BSR 发送 Bootstrap 自举消息的间隔时间”，否则，将导致 BSR 选举不稳定。

----结束

5.5.4 配置 BSR 服务边界

可以在接口上配置 BSR 服务边界，Bootstrap 消息无法通过 BSR 服务边界。众多 BSR 边界接口将网络划分成不同的 PIM-SM 域。

背景信息

在有待成为 BSR 服务边界的路由器上进行如下配置。

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 bsr-boundary**，配置 BSR 服务边界。BSR 消息无法通过 BSR 区域边界。

缺省情况下，网络中的所有 PIM-SM 路由器都能收到 BSR 消息。

----结束

5.5.5 （可选）配置合法 BSR 的地址范围

在所有设备上通过 ACL 设置 C-BSR 地址的过滤策略，只有 Bootstrap 消息的源地址在合法地址范围内时，才接收 Bootstrap 消息，从而防止 BSR 欺骗。

背景信息

在 PIM-SM 域中所有路由器上进行如下配置。

说明

缺省情况下,不检查 BSR 报文源地址,一律接收。

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** ，进入 PIM 视图。

步骤 3 执行命令 **bsr-policy** { *basic-acl-number* | **acl-name** *acl-name* }，限定合法 BSR 地址范围。当路由器接收到封装了 Bootstrap 消息的 IP 报文时，检查报文源地址。如果源地址在合法地址范围之外，则丢弃该报文，从而防止 BSR 欺骗。

{ *basic-acl-number* | **acl-name** *acl-name* }为访问控制列表，该列表定义了针对 BSR 报文源地址范围的过滤策略。

----结束

5.5.6 （可选）配置合法 C-RP 的地址范围

在所有 C-BSR 上通过 ACL 设置 C-RP 地址和 C-RP 所服务的组地址的过滤策略，只有 C-RP 地址和所服务的组地址都在合法地址范围内时，才将 C-RP 信息收入 RP-Set，从而防止 C-RP 欺骗。

背景信息

在 PIM-SM 域中所有 C-BSR 上进行如下配置。

说明

缺省情况下，不检查 Advertisement 消息包含的 C-RP 地址和所服务的组地址，一律收入 RP-Set。

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** ，进入 PIM 视图。

步骤 3 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。当路由器接收到 Advertisement 消息时，检查消息中包含的 C-RP 地址和所服务的组地址。只有 C-RP 地址和所服务的组地址都在合法地址范围之内时，才收入 RP-Set，从而防止 C-RP 欺骗。

{ *advanced-acl-number* | **acl-name** *acl-name* }：表示高级访问控制列表，该列表定义了针对 C-RP 地址范围及其服务组地址范围的过滤策略。

----结束

5.5.7 检查配置结果

调整 C-RP 和 C-BSR 的控制参数成功后，可以通过命令查看 BSR 和 RP 的信息，接口上是否配置了 BSR 服务边界。

操作步骤

- 使用 **display pim bsr-info** 命令查看 PIM-SM 域中 BSR 自举路由器的信息。
- 使用 **display pim rp-info** [*group-address*]命令查看 PIM-SM 域中的 RP 信息。

----结束

5.6 配置 BSR 管理域

将 PIM-SM 网络划分为多个 BSR 管理域和一个 Global 域，可以分担单一 BSR 的管理压力，还可以使用私有组地址为特定区域的用户提供专门服务。

5.6.1 建立配置任务

使用动态 RP 配置 PIM-SM 基本功能后，可以根据实际需要配置 BSR 管理域。每个 BSR 管理域中维护一个 BSR，为特定范围的组播组服务，不属于任何 BSR 管理域的组播组，都属于 Global 域的服务范围。本节介绍在 ASM 模型中如何通过命令配置 BSR 管理域。

应用环境

缺省情况下，PIM-SM 网络中只有一个 BSR，整个网络都在该 BSR 的管理范围内。为了更好的、有针对性地管理网络，可以在 PIM-SM 网络中设置多个 BSR 管理域。每个 BSR 管理域中维护一个 BSR，为特定范围的组播组服务，属于此范围的组播报文无法通过 BSR 管理域边界。

不同的 BSR 管理域服务的组播组范围可以重叠，该组播组只在本管理域内有效，相当于私有组地址。

不属于任何 BSR 管理域的组播组，一律属于 Global 域的服务范围。Global 域中维护一个 BSR，为所有剩余的组播组服务。

将一个统一的 PIM-SM 网络划分为多个 BSR 管理域和一个 Global 域，一方面有效分担单一 BSR 的管理压力，另一方面可以使用私有组地址为特定区域提供专门服务。

路由器在系统缺省值的控制下可以正常的工作。同时，AR2200-S 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在配置 BSR 管理域之前，需完成以下任务：

- 配置单播路由协议
- **配置 PIM-SM 基本功能**

数据准备

在配置 BSR 管理域之前，需准备以下数据。

序号	数据
1	PIM-SM 某管理域候选 BSR 的优先级和哈希掩码长度
2	Global 域候选 BSR 的优先级和哈希掩码长度

5.6.2 使能 BSR 管理域

在 PIM-SM 网络中所有设备上使能 BSR 管理域功能。

背景信息

在 PIM-SM 网络中所有路由器上进行如下配置。

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** ，进入 PIM 视图。

步骤 3 执行命令 **c-bsr admin-scope**，使能在 PIM-SM 网络的中划分 BSR 管理域。

----结束

5.6.3 配置 BSR 管理域边界

在接口上配置 BSR 管理域边界后，属于该 BSR 管理域的组播报文无法通过此边界。

背景信息

在有待成为 BSR 服务边界的路由器上进行如下配置。

说明

BSR 管理域边界之外的路由器不能转发属于此 BSR 管理域的组播报文。

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 **multicast boundary** *group-address* { *mask* | *mask-length* }，配置 BSR 管理域边界。属于该 BSR 管理域的组播报文无法通过此边界。

----结束

5.6.4 调整 C-BSR 参数

可以根据实际需要调整 BSR 管理域和 Global 域的 C-BSR 参数。

背景信息

在所有 C-BSR 上进行如下配置。

说明

C-BSR 参数在三种情况配置：

- 全局。请参见**调整 C-RP 和 C-BSR 的控制参数**。全局值在 Global 域和各 BSR 域中都有效。
- BSR 管理域。针对 BSR 管理域的取值优于全局值，未配置 BSR 管理域值时继承全局值。
- Global 域。针对 Global 域的取值优于全局值，未配置 Global 域值时继承全局值。

操作步骤

- BSR 管理域
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，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 参数。
     - *group-address* { *mask* | *mask-length* }为 C-BSR 服务的组播组范围。有效的组范围在 239.0.0.0/8 之内。
     - **hash-length** *hash-length* 为 C-BSR 的哈希掩码长度。
     - **priority** *priority* 为 C-BSR 的优先级。

- Global 域
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **c-bsr global** [**hash-length** *hash-length* | **priority** *priority*] *，配置 C-BSR 参数。
     - **hash-length** *hash-length* 为 C-BSR 的哈希掩码长度。
     - **priority** *priority* 为 C-BSR 的优先级。

----结束

5.6.5 检查配置结果

配置 BSR 管理域成功后，可以通过命令查看 BSR 和 RP 的信息。

操作步骤

- 使用 **display pim bsr-info** 命令查看 PIM-SM 域中 BSR 的信息。
- 使用 **display pim rp-info** [*group-address*]命令查看 PIM-SM 域中的 RP 信息。

----结束

5.7 调整邻居控制参数

设备间通过交互 Hello 消息建立 PIM 邻居关系，协商各类控制参数。可以根据实际需要调整 Hello 消息中携带的参数，若无特殊要求推荐采用缺省值。

5.7.1 建立配置任务

配置 PIM-SM 基本功能后，可以根据实际需要调整 Hello 消息的相关参数来控制邻居关系，配置跟踪下游邻居和邻居过滤功能。

应用环境

本节所有配置同时适用于 ASM 模型和 SSM 模型。

PIM 路由器之间通过交互 Hello 消息建立邻居关系，协商各类控制参数，并选举 DR。

路由器在系统缺省值的控制下可以正常的工作。同时，AR2200-S 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在配置邻居控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-SM 基本功能**

数据准备

在调整邻居控制参数之前，需准备以下数据。

序号	数据
1	竞选 DR 的优先级
2	等待接收邻居发送 Hello 消息的超时时间
3	发送 Hello 消息的时间间隔
4	触发 Hello 消息的最大延迟
5	DR 切换延迟，即当接口由 DR 变成非 DR 时，原有表项仍然有效的时间
6	过滤 PIM 邻居的 ACL 号或 ACL 名字

5.7.2 配置 PIM 邻居控制参数

配置 PIM 邻居控制参数可以在全局和接口两种情况下配置。接口配置优于 PIM 视图下的配置，接口上未配置时 PIM 视图下的配置生效。

背景信息

在 PIM-SM 路由器上进行如下配置。

说明

PIM 邻居的控制参数可以在两种情况下配置：

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **timer hello** *interval*，配置发送 Hello 消息的时间间隔。
  4. 执行命令 **hello-option holdtime** *interval*，配置保持邻居为可达状态的超时时间，若超时仍没有收到 Hello 消息则认为邻居不可达。
- 接口
  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 **pim timer hello** *interval*，配置发送 Hello 消息的时间间隔。
  4. 执行命令 **pim triggered-hello-delay** *interval*，配置触发 Hello 消息的最大延迟，避免多个 PIM 路由器同时发送 Hello 消息而导致冲突。
  5. 执行命令 **pim hello-option holdtime** *interval*，配置保持邻居为可达状态的超时时间，若超时仍没有收到 Hello 消息则认为邻居不可达。

6. 执行命令 **pim require-genid**，配置接收的 Hello 消息中应包含 Generation ID 选项，拒绝无 Generation ID 选项的 Hello 消息。

   缺省情况下，路由器接受无 Generation ID 选项的 Hello 消息。

----结束

5.7.3 配置竞选 DR 的控制参数

竞选 DR 的控制参数可以在全局和接口两种情况下配置。

背景信息

在 PIM-SM 路由器上进行如下配置。

说明

竞选 DR 的控制参数可以在两种情况下配置：

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **hello-option dr-priority** *priority*，配置竞选 DR 的优先级。

     当同一网段内的所有 PIM 路由器都支持 DR 优先级的时候，由优先级较高的路由器接口充当 DR，优先级相同时由 IP 地址较大的路由器接口充当 DR；只要有一台 PIM 路由器不支持 DR 优先级，则由 IP 地址较大的路由器接口充当 DR。
- 接口
  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 **pim hello-option dr-priority** *priority*，配置竞选 DR 的优先级。

     当同一网段内的所有 PIM 路由器都支持 DR 优先级的时候，由优先级较高的路由器接口充当 DR，优先级相同时由 IP 地址较大的路由器接口充当 DR；只要有一台 PIM 路由器不支持 DR 优先级，则由 IP 地址较大的路由器接口充当 DR。
  4. 执行命令 **pim timer dr-switch-delay** *interval*，配置 DR 切换延迟，并指定延迟时间。当接口由 DR 变成非 DR 时，原有表项仍然有效直到延迟时间超时。

     缺省情况下，当接口由 DR 变为非 DR 时，立即删除 PIM 路由表项。

----结束

5.7.4 使能跟踪下游邻居功能

当来自上游的 Hello 消息中的 Generation ID 发生改变，则表明上游邻居状态发生改变。可以配置 PIM 接口拒绝无 Generation ID 参数的 Hello 消息，从而实时了解上游邻居的状态。

背景信息

在运行 PIM-SM 的路由器上进行如下配置。

说明

配置跟踪下游邻居功能可以在两种情况下配置:

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **hello-option neighbor-tracking**，使能跟踪下游邻居功能，记录已经发送了加入报文并且该加入状态还没有超时的下游邻居信息。

     说明

     除非共享网段中的所有 PIM 路由器都使能该能力，否则邻居跟踪功能无法实现。
- 接口
  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 **pim hello-option neighbor-tracking**，使能跟踪下游邻居功能，记录已经发送了加入报文并且该加入状态还没有超时的下游邻居信息。

     说明

     除非共享网段中的所有 PIM 路由器都使能该能力，否则邻居跟踪功能无法实现。

----结束

5.7.5 配置邻居过滤

为了防止未知设备参与 PIM 协议，需要过滤 PIM 邻居。接口上只与符合过滤规则的地址建立邻居关系，删除不符合过滤规则的邻居。

背景信息

为了防止未知路由器参与 PIM 协议，阻止本路由器成为 DR，需要过滤 PIM 邻居。

在运行 PIM-SM 的路由器上进行如下配置。

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* }，配置邻居过滤。

接口上只与符合过滤规则的地址建立邻居关系，删除不符合过滤规则的邻居。

说明

在接口上配置邻居过滤功能时，与该接口建立 PIM 邻居的路由器上都需要配置相应的邻居过滤功能。

----结束

5.7.6 检查配置结果

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

----结束

5.8 调整源注册控制参数

与组播源直连的 DR 将接收到的组播数据逐一封装到 Register 消息中，以单播方式发送到 RP。RP 将解封装后的组播数据沿 RPT 转发到接收者。系统允许配置 Register 消息过滤和注册抑制功能。

5.8.1 建立配置任务

配置 PIM-SM 基本功能后，可以根据实际需要配置 Register 消息的过滤规则和校验方式，配置注册抑制。

应用环境

本节介绍在 ASM 模型中如何通过命令配置源注册控制参数。

在 PIM-SM 网络中，与组播源 S 直连的 DR 将接收到的组播数据逐一封装到 Register 消息中，以单播方式发送到 RP。RP 将解封装后的组播数据沿 RPT 转发到接收者。

当 RP 上的 SPT 切换完成后，组播数据以组播方式沿 SPT 到达 RP。这时，RP 向组播源侧 DR 发送 Register-stop 消息，DR 停止发送 Register 注册消息并进入注册抑制状态。在注册抑制期间，DR 向 RP 周期性的发送空注册消息以通告组播源仍处于激活状态；注册抑制超时后，DR 重新开始发送 Register 注册消息。

路由器在系统缺省值的控制下可以正常的工作。同时，AR2200-S 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在配置源注册控制参数之前，需完成以下任务：

- 配置某单播路由协议

- 配置 PIM-SM 基本功能

数据准备

在配置源注册控制参数之前，需准备以下数据：

序号	数据
1	RP 过滤 Register 注册报文的 ACL 规则
2	是否仅根据 Register 注册报文头信息计算校验和
3	保持 Register 注册抑制状态的超时时间
4	向 RP 发送空 Register 注册消息的时间间隔
5	源 DR 发送注册报文的接口类型和接口号

5.8.2 配置 PIM-SM 注册报文

可以在所有可能成为 RP 的设备上，配置 Register 消息过滤规则。缺省情况下根据整个 Register 消息来计算校验和，可以配置仅根据 Register 注册消息头信息来计算校验和。

背景信息

在所有可能成为 RP 的路由器上进行如下配置。

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** ，进入 PIM 视图。

步骤 3 执行命令 **register-policy** { *advanced-acl-number* | **acl-name** *acl-name* }，配置过滤 Register 注册报文的规则。RP 根据此规则来过滤接收到的注册报文。

步骤 4 执行命令 **register-header-checksum**，配置仅根据 Register 注册消息头信息来计算校验和。未通过校验的 Register 注册消息将被丢弃。缺省情况下根据整个消息来计算校验和。

----结束

5.8.3 配置 PIM-SM 注册抑制

可以在所有可能成为组播源侧 DR 的设备上，配置保持注册抑制状态的超时时间和发送空注册消息的时间间隔。

背景信息

在所有可能成为组播源侧 DR 的路由器上进行如下配置。

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** ，进入 PIM 视图。

步骤 3 执行命令 **register-suppression-timeout** *interval*，配置保持注册抑制状态的超时时间。

步骤 4 执行命令 **probe-interval** *interval*，配置发送空注册消息的时间间隔。

说明

probe-interval 的值必须小于 **register-suppression-timeout** 值的二分之一。

----结束

5.8.4 检查配置结果

调整源注册控制参数成功后，可以通过命令查看 PIM 接口信息。

操作步骤

步骤 1 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看接口上的 PIM 信息。

----结束

5.9 调整转发控制参数

设备向上游发送 Join 消息请求转发组播数据，发送 Prune 消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。

5.9.1 建立配置任务

配置 PIM-SM 基本功能后，可以根据实际需要调整维护转发关系的控制参数，配置 Join 信息过滤和邻居检查功能来提高安全性。

应用环境

若无特殊说明，本节各项配置同时适用于 ASM 模型和 SSM 模型。

当路由器上出现第一个组成员时，路由器从上游接口发出 Join 消息，请求上游路由器向该网段转发组播报文。

当路由器上的最后一个组成员离开时，路由器从上游接口发出 Prune 消息，请求上游路由器执行剪枝操作，停止向该网段转发组播报文。当该网段中还存在其他下游路由器时，其他下游路由器必须发送 Join 消息，否决剪枝操作。

在 ASM 模型中，路由器周期性的向 RP 发送 Join 消息，避免 RPT 分支因为超时而被删除。

路由器在系统缺省值的控制下可以正常的工作。同时，AR2200-S 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在调整转发控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-SM 基本功能**

数据准备

在调整转发控制参数之前，需准备以下数据。

序号	数据
1	发送 Join/Prune 消息的时间间隔
2	保持加入/剪枝状态的时间
3	传递消息的延迟时间
4	否决剪枝的时间
5	过滤 Join 信息的 ACL 号或 ACL 名字
6	接收或发送 Join/Prune 报文和 Assert 报文时，是否进行邻居检查

5.9.2 配置维持转发关系的控制参数

转发控制参数可以在全局和接口两种情况下配置。转发控制参数包括：发送 Join/Prune 消息的周期和下游接口保持 Join/Prune 状态的时间。

背景信息

在 PIM-SM 路由器上进行如下配置。

说明

维持转发关系的控制参数可以在两种情况下配置：

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **timer join-prune** *interval*，配置发送 Join/Prune 消息的时间间隔。
  4. 执行命令 **holdtime join-prune** *interval*，配置下游接口保持加入/剪枝状态的时间。
- 接口
  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 **pim timer join-prune** *interval*，配置发送 Join/Prune 消息的时间间隔。
4. 执行命令 **pim holdtime join-prune** *interval*，配置下游接口保持加入/剪枝状态的时间。
5. 执行命令 **pim require-genid**，配置接收的 Hello 消息中应包含 Generation ID 选项，拒绝无 Generation ID 选项的 Hello 消息。

   当来自上游的 Hello 消息中的 Generation ID 发生改变，则表明上游邻居丢失或上游邻居状态已经改变。路由器立即向上游发送 Join/Prune 消息进行状态刷新。

   缺省情况下，路由器接受无 Generation ID 选项的 Hello 消息。

----结束

5.9.3 配置剪枝控制参数

剪枝控制参数可以在全局和接口两种情况下配置。剪枝控制参数包括：在 LAN 内传输消息的延迟时间和否决剪枝的时间间隔。

背景信息

在 PIM-SM 路由器上进行如下配置。

说明

剪枝的控制参数可以在两种情况下配置:

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **hello-option lan-delay** *interval*，配置在 LAN 内传输消息的延迟时间。

     Hello 消息携带 lan-delay（消息传输延迟时间）参数和 override-interval（否决剪枝时间）参数。PPT 表示路由器从下游接口收到剪枝消息到执行剪枝操作（抑制下游接口转发）之间的延时。lan-delay + override-interval ＝ PPT。如果在 PPT 时间内下游接口收到 Join 消息，则取消剪枝操作。
  4. 执行命令 **hello-option override-interval** *interval*，配置否决剪枝的时间。

     当同一网段中有路由器向上游发送剪枝消息时，如果其他路由器仍然需要接收组播数据，则必须在 override-interval 时间内向上游发送 Join 消息。
- 接口
  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 **pim hello-option lan-delay** *interval*，配置在 LAN 内传输消息的延迟时间。
  4. 执行命令 **pim hello-option override-interval** *interval*，配置否决剪枝的时间。

----结束

5.9.4 配置 Join 信息过滤

接口上接收的 Join/Prune 消息中包含 Join 信息和 Prune 信息。可以通过配置 ACL 来过滤 Join 信息，设备根据符合过滤规则的 Join 信息建立 PIM 表项。

背景信息

接口上接收的 Join/Prune 消息中包含 Join 信息和 Prune 信息。可以通过配置 ACL 来过滤 Join 信息，路由器根据符合过滤规则的 Join 信息建立 PIM 表项，从而防止非法用户加入。

在运行 PIM-SM 的路由器上进行如下配置。

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。

----结束

5.9.5 配置邻居检查功能

接收或发送 Join/Prune 消息和 Assert 消息时，检查该消息是否来自 PIM 邻居或发送给 PIM 邻居，如果不是则不处理。

背景信息

缺省情况下，接收或发送 Join/Prune 消息和 Assert 消息时，不检查该消息是否来自 PIM 邻居或发送给 PIM 邻居。

如果需要配置 PIM 邻居检查功能，建议在与用户相连的设备上配置，在网络内部设备上不推荐使用此功能。接收或发送 Join/Prune 消息和 Assert 消息时，检查该消息是否来自 PIM 邻居或发送给 PIM 邻居，如果是则处理，否则丢弃。

在运行 PIM-SM 的路由器上进行如下配置。

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** ，进入 PIM 视图。

步骤 3 执行命令 **neighbor-check** { **receive** | **send** }，配置邻居检查功能。

可以同时使能接收和发送 Join/Prune 消息和 Assert 消息时的邻居检查功能。

说明

只有 AR2200-SHI 支持此命令。

----结束

5.9.6 检查配置结果

调整转发控制参数成功后，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 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看接口上的 PIM 信息。
- 使用 **display pim control-message counters** [**message-type** { **assert** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** | **bsr** } | **interface** *interface-type interface-number*] * 命令查看发送和接收 PIM 控制报文的数目信息。
- 使用以下命令查看 PIM 路由表：
  - **display pim 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 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

5.10 调整 Assert 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 消息，参与竞选唯一上游。

5.10.1 建立配置任务

配置 PIM-SM 基本功能后，可以根据实际需要配置保持 Assert 状态的时间。

应用环境

本节所有配置项同时适用于 ASM 模型和 SSM 模型。

当 PIM-SM 路由器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路由器。路由器从该接口发出 Assert 消息，参与竞选唯一上游。

路由器在系统缺省值的控制下可以正常的工作。同时，AR2200-S 允许用户根据具体环境，适当调整相关参数。

说明

如果实际网络没有特殊要求，推荐采用缺省值。

前置任务

在调整 Assert 控制参数之前，需完成以下任务：

- 配置某单播路由协议
- **配置 PIM-SM 基本功能**

数据准备

在调整 Assert 控制参数之前，需准备以下数据。

序号	数据
1	保持 Assert 状态的时间

5.10.2 配置保持 Assert 状态的时间

落选设备保持 Assert 状态的时间内禁止下游接口转发组播数据，超时后恢复转发。

背景信息

在 PIM-SM 域内所有路由器上进行如下配置。

说明

Assert 控制参数可以在两种情况下配置：

- 全局。在各接口上都有效。
- 接口。针对接口的取值优于全局值，未配置接口值时继承全局值。

操作步骤

- 全局
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **pim** ，进入 PIM 视图。
  3. 执行命令 **holdtime assert** *interval*，配置保持 Assert 状态的时间。落选路由器在此时间内禁止下游接口转发组播数据，超时后恢复转发。
- 接口
  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 **pim holdtime assert** *interval*，配置保持 Assert 状态的时间。落选路由器在此时间内禁止下游接口转发组播数据，超时后恢复转发。

----结束

5.10.3 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 控制消息统计数和 PIM 路由表等信息。

操作步骤

- 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看接口上的 PIM 信息。

- 使用 **display pim control-message counters** [**message-type** { **assert** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** | **bsr** } | **interface** *interface-type interface-number*] * 命令查看发送和接收 PIM 控制报文的数目信息。
- 使用以下命令查看 PIM 路由表：
  - **display pim 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 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

5.11 配置基于 PIM 协议的 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。

5.11.1 建立配置任务

基于 PIM 协议的 Anycast RP 适用于单 PIM-SM 域，在配置此特性之前，请保证 PIM-SM 域内组播网络畅通。

应用环境

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。

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。

基于 PIM 协议的 Anycast RP 适用于单 PIM-SM 域，若需要获取 PIM-SM 域外的源组信息，可通过以下两种方案实现：

- PIM-SM 域内所有 Anycast RP 成员都与外部建立 MSDP 对等体。
- 将 PIM-SM 域内的 Anycast RP 分为两部分，一部分与外部建立 MSDP 对等体，另一部分不建立 MSDP 对等体，当与外部建立 MSDP 对等体的 RP 收到 MSDP SA 消息时，转换为注册报文发送给其他未建立 MSDP 对等体的 RP。

说明

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
- **配置 PIM-SM 基本功能**

数据准备

在配置基于 PIM 协议的 Anycast RP 之前，需准备以下数据。

序号	数据
1	Anycast RP 地址
2	Anycast RP 本地地址

5.11.2 配置全局 Anycast RP

在 PIM-SM 域内有待建立 Anycast RP 的多台设备上，配置相同的当选 RP 地址作为 Anycast RP 地址。

背景信息

说明

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。

在 PIM-SM 域内有待建立 Anycast RP 的多台路由器上，分别进行如下配置。

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** ，进入 PIM 视图。

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

说明

请将 Anycast RP 地址配置为与网络中的 RP 地址相同。

----结束

5.11.3 配置 Anycast RP 本地地址

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

背景信息

在 PIM-SM 域内 Anycast RP 上进行如下配置。

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**，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

Anycast RP 本地地址必须是现有实例某个接口的 IP 地址。

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

5.11.4 配置 Anycast RP 对等体

向 Anycast RP 对等体转发注册报文时，需要将目的地址转换为 Anycast RP 对等体地址。

背景信息

在 PIM-SM 域内 Anycast RP 上进行如下配置。

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**，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。

- *peer-address* 即 Anycast RP 对等体的本地地址。
- 若指定 **fwd-msdp-sa** 参数，则将接收到的 MSDP SA 消息提取源组信息后封装成注册报文向 Anycast RP 对等体转发。

说明

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

5.11.5 检查配置结果

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。

前提条件

已经完成基于 PIM 协议的 Anycast RP 功能的所有配置。

操作步骤

- 使用 **display pim rp-info** 命令查看 RP 信息。
- 使用 **display pim routing-table** 命令查看 PIM 路由表信息。

----结束

任务示例

在 Anycast RP 上执行命令 **display pim rp-info**，查看是否存在相同的 RP 信息。

```
<Huawei> display pim rp-info
 VPN-Instance: public net
 PIM-SM BSR RP Number:1
 Group/MaskLen: 224.0.0.0/4
     RP: 1.1.1.1 (local)
     Priority: 0
     Uptime: 00:45:19
     Expires: 00:02:11
```

若在 Anycast RP 上均已存在相同的 RP 信息，如举例中的显示信息“**RP: 1.1.1.1 (local)**”，则 Anycast RP 配置成功。

在 Anycast RP 上执行命令 **display pim routing-table**，查看 PIM 路由表信息。

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

 (10.110.1.2, 226.1.1.1)
     RP: 1.1.1.1 (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
```

若在 Anycast RP 上均已存在相同的 RP 信息，如举例中的显示信息“**RP: 1.1.1.1 (local)**”，则 Anycast RP 配置成功。

5.12 配置防止主机恶意攻击功能（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。

5.12.1 建立配置任务

网络中 PIM-SM 和 IGMP 的基本功能都已配置后，将 PIM Silent 特性配置在与主机相连的接口上，该接口使能了 PIM-SM 和 IGMP。

应用环境

在接入层上，路由器直连用户主机的接口上需要使能 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，有可能导致路由器瘫痪。

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路由器接口，且该用户网段只与这一台路由器相连。

注意

如果在与路由器相连的接口上启动该功能，将导致 PIM 邻居无法正常建立，引发组播故障。

如果用户网段与多台路由器相连，在多个路由器接口上配置 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。

前置任务

在配置防止主机恶意攻击功能之前，需要完成以下任务：

- 配置单播路由协议，使网络畅通。
- 配置 PIM-SM
- 配置 IGMP

数据准备

在配置防止主机恶意攻击功能之前，需要准备以下数据。

序号	数据
1	与用户主机相连的路由器接口类型和编号

5.12.2 配置 PIM Silent

配置 PIM Silent 后，接口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，并自动成为 DR。同时，该接口上的 IGMP 功能不受影响。

背景信息

在与用户主机网段直连的接口上进行如下配置。

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。可以有效的防范恶意主机 Hello 报文攻击，保护路由器。

----结束

5.12.3 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。

前提条件

已经完成防止主机恶意攻击功能（PIM Silent）功能的所有配置。

操作步骤

步骤 1 使用 **display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]命令查看 PIM 接口信息。

----结束

任务示例

执行命令 **display pim interface verbose**，可以看到使能了此配置。

```
<RouterA> display pim interface verbose
 VPN-Instance: public net
 Interface: GigabitEthernet1/0/0, 2.2.2.2
     PIM version: 2
     PIM mode: Sparse
     PIM state: up
     PIM DR: 10.1.2.2 (local)
     PIM DR Priority (configured): 1
     PIM neighbor count: 0
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM hello override interval (negotiated): 2500 ms
     PIM hello override interval (configured): 2500 ms
     PIM Silent: enabled
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM generation ID: 0X4B9F5B92
     PIM require-GenID: disabled
     PIM hello hold interval: 105 s
     PIM assert hold interval: 180 s
     PIM triggered hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM BSR domain border: disabled
     PIM BFD: disabled
     PIM dr-switch-delay timer : not configured
     Number of routers on link not using DR priority: 0
     Number of routers on link not using LAN delay: 0
     Number of routers on link not using neighbor tracking: 1
     ACL of PIM neighbor policy: -
     ACL of PIM ASM join policy: -
     ACL of PIM SSM join policy: -
     ACL of PIM join policy: -
```

5.13 维护 PIM-SM（IPv4）

PIM-SM 的维护包括：清除 PIM 统计信息。

5.13.1 清除 PIM 控制报文统计信息

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。

背景信息

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

步骤 1 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 control-message counters** [**interface** *interface-type interface-number*]命令。

----结束

5.13.2 清除 PIM 表项的指定下游接口的 PIM 状态

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

背景信息

注意

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

该命令用来清除非法用户的加入信息，可清除指定表项指定接口的 PIM 状态，如：PIM 加入/剪枝状态，Assert 状态。

该命令不清除指定接口的 IGMP 或静态组的加入状态。

操作步骤

步骤 1 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 routing-table group** *group-address* **mask** { *group-mask-length* | *group-mask* } **source** *source-address* **interface** *interface-type interface-number* 命令。

----结束

5.14 配置举例

通过配置举例，可以了解如何构建基本的 PIM-SM 网络、配置 PIM-SM 常用功能。

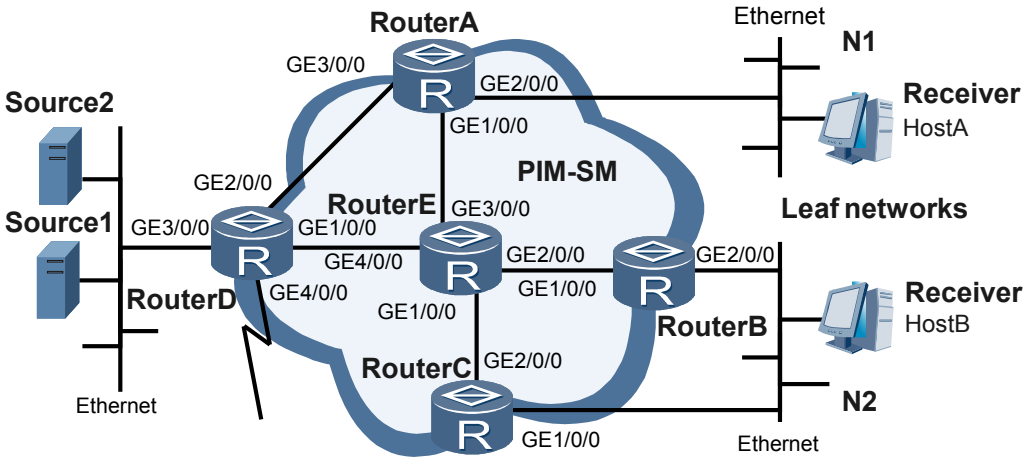
5.14.1 配置 PIM-SM 组播网络示例

在单播路由正常的 AS 内配置 PIM-SM 基本功能，使用户能够接收任意组播源发送的数据。

组网需求

在如图 5-2 所示的 ISP 网络中部署组播业务。已知该网络中已经部署了完备的 IGP，单播运行正常，并接入 Internet。要求通过在路由器上进行适当配置，使网络中的用户主机能够通过组播方式接收视频信息。

图 5-2 配置 PIM-SM 典型组播网络组网图



Device	接口	IP 地址
RouterA	GE1/0/0	192.168.9.1/24
	GE3/0/0	192.168.1.1/24
	GE2/0/0	10.110.1.1/24
RouterB	GE1/0/0	192.168.2.1/24
	GE2/0/0	10.110.2.1/24
RouterC	GE2/0/0	192.168.3.1/24
	GE1/0/0	10.110.2.2/24
RouterD	GE1/0/0	192.168.4.2/24
	GE2/0/0	192.168.1.2/24
	GE4/0/0	10.110.4.1/24
	GE3/0/0	10.110.5.1/24
RouterE	GE1/0/0	192.168.3.2/24
	GE2/0/0	192.168.2.2/24
	GE3/0/0	192.168.9.2/24
	GE4/0/0	192.168.4.1/24

配置思路

由于 ISP 网络接入 Internet，为了易于业务拓展，采用 PIM-SM 协议配置组播功能，同时使用 ASM 和 SSM 模型提供组播服务。

1. 配置各路由器的接口 IP 地址和单播路由协议。组播域内路由协议 PIM 是依赖单播路由协议，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 IP 组播路由功能。使能 IP 组播路由功能是配置 PIM-SM 的前提。

3. 在组播路由器的所有接口上使能 PIM-SM 功能。使能 PIM-SM 功能之后才能配置 PIM-SM 的其他功能。

   说明

   如果该接口下还需要配置 IGMP 协议，必须先使能 PIM-SM，才能使能 IGMP 协议。两者顺序不能颠倒，否则 PIM-SM 功能配置会不成功。

4. 在与主机侧相连的路由器接口上使能 IGMP。接受者能通过发送 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。
5. 在与直连用户主机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，增加组播路由器的安全性。

   说明

   该功能仅适用于与用户主机网段直连的路由器接口，且该用户网段只与这一台路由器相连。

6. 配置 RP。在 PIM-SM 网络中，RP 是 RPT 树的根节点。建议 RP 的位置配置在组播流量分支较多的路由器上，如本图中的 RouterE 的位置。

   说明

   - 用户侧的 DR 得到新的 IGMP 成员关系创建(*,G)表项后，向 RP 发送加入/剪枝消息，沿路更新共享树。
   - 组播数据源刚开始向组发送数据时，由其 DR 向 RP 单播发送注册消息，RP 将其解封装后沿共享树分发给其组成员，同时 RP 向组播源侧 DR 发送注册-停止消息。

7. （可选）在与 Internet 相连的接口上配置 BSR 边界，Bootstrap 消息不能通过该边界，使 BSR 只为该 PIM-SM 域服务，增加组播可控性。
8. （可选）在各路由器设置 SSM 组地址范围。使 PIM-SM 域内的组播路由器只为 SSM 组地址范围内的组播组服务，实现可控组播。

数据准备

为完成此配置举例，需准备如下的数据：

- 组播组 G1 地址：225.1.1.1/24。
- 组播组 G2 地址：227.1.1.1/24。
- 组播源 S1 地址：10.110.5.100/24。
- 组播源 S2 地址：10.110.6.100/24。
- 路由器接口和用户主机之间运行的 IGMP 版本号为 3。

操作步骤

步骤 1 配置各路由器的接口 IP 地址和单播路由协议

按照图 5-2 配置各路由器接口的 IP 地址和掩码，配置各路由器之间采用 OSPF 进行互连，确保网络中各路由器 RouterA、RouterB、RouterC、RouterD、RouterE 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。具体配置过程略，详见配置文件。

步骤 2 使能 IP 组播路由功能，在各接口上使能 PIM-SM 功能

在所有路由器上使能组播功能，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，详见配置文件。

```
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 2/0/0
```

```
[RouterA-GigabitEthernet2/0/0] pim sm
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] pim sm
[RouterA-GigabitEthernet1/0/0] 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，详见配置文件。

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] igmp enable
[RouterA-GigabitEthernet2/0/0] igmp version 3
```

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。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。

本示例同时配置两种 RP，并通过参数配置，优选动态 RP，静态 RP 作为备份。

配置动态 RP，需要在 PIM-SM 域的一个或多个路由器上进行如下配置。本例中在 RouterE 上配置 RP 通告的服务范围，及 C-BSR 和 C-RP 的位置。

```
[RouterE] acl number 2005
[RouterE-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[RouterE-acl-basic-2005] quit
[RouterE] pim
[RouterE-pim] c-bsr gigabitethernet 3/0/0
[RouterE-pim] c-rp gigabitethernet 3/0/0 group-policy 2005 priority 0
```

配置静态 RP，需要在所有组播路由器上配置。本例中需要在 RouterA、RouterB、RouterC、RouterD 和 RouterE 上进行如下配置。RouterB、RouterC、RouterD 和 RouterE 上的配置过程与 RouterA 上的配置相似，配置过程略，详见配置文件。

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 4/0/0
[RouterD-GigabitEthernet4/0/0] pim bsr-boundary
[RouterD-GigabitEthernet4/0/0] quit
```

步骤 7 配置 SSM 组播组地址范围

在所有路由器上配置 SSM 组播组地址范围为 227.1.1.0/24。RouterB、RouterC、RouterD 和 RouterE 上的配置过程与 RouterA 上的配置完全相同，配置过程略，详见配置文件。

```
[RouterA] acl number 2000
[RouterA-acl-basic-2000] rule permit source 227.1.1.0 0.0.0.255
[RouterA-acl-basic-2000] quit
[RouterA] pim
```

```
[RouterA-pim] ssm-policy 2000
```

步骤 8 检验配置效果

通过使用 **display pim interface** 命令可以查看路由器接口上 PIM 的配置和运行情况。例如 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          192.168.3.1
```

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: 192.168.9.2
     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: 192.168.9.2
     Priority: 0
     Hash 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: 192.168.9.2
     Priority: 0
     Hash mask length: 30
     State:Elected
     Scope: Not scoped
     Wait to be BSR: 0
```

通过使用 **display pim rp-info** 命令可以查看路由器上获取的 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 information:
 Group/MaskLen: 225.1.1.0/24
     RP: 192.168.9.2
     Priority: 0
     Uptime: 00:45:13
     Expires: 00:02:17
 PIM SM static RP information:
     Static RP: 192.168.2.2
```

通过使用 **display pim routing-table** 命令可以查看路由器 PIM 协议组播路由表。HostA 需要接收组播组（225.1.1.1/24）信息，HostB 需要接收组播源（10.110.5.100/24）发往组播组（227.1.1.1/24）的信息。显示信息如下：

```
<RouterA> display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry
(*, 225.1.1.1)
```

```
    RP: 192.168.9.2
    Protocol: pim-sm, Flag: WC
    UpTime: 00:13:46
    Upstream interface: GigabitEthernet1/0/0,
        Upstream neighbor: 192.168.9.2
        RPF neighbor: 192.168.9.2
    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: 192.168.9.2
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 00:00:42
    Upstream interface: GigabitEthernet3/0/0
        Upstream neighbor: 192.168.1.2
        RPF neighbor: 192.168.1.2
   Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/0/0
            Protocol: pim-sm, UpTime: 00:00:42, Expires:-
(10.110.6.100, 225.1.1.1)
    RP: 192.168.9.2
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 00:00:42
    Upstream interface: GigabitEthernet3/0/0
        Upstream neighbor: 192.168.1.2
        RPF neighbor: 192.168.1.2
   Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/0/0
            Protocol: pim-sm, UpTime: 00:00:42, Expires:-
<RouterD> display pim routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 2 (S, G) entries
 (10.110.5.100, 225.1.1.1)
    RP: 192.168.9.2
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 00:00:42
    Upstream interface: GigabitEthernet3/0/0
        Upstream neighbor: 10.110.5.100
        RPF neighbor: 10.110.5.100
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/0/0
            Protocol: pim-sm, UpTime: 00:00:42, Expires:-
 (10.110.6.100, 225.1.1.1)
    RP: 192.168.9.2
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 00:00:42
    Upstream interface: GigabitEthernet3/0/0
        Upstream neighbor: 10.110.5.100
        RPF neighbor: 10.110.5.100
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/0/0
            Protocol: pim-sm, UpTime: 00:00:42, Expires:-
(10.110.5.100, 227.1.1.1)
    Protocol: pim-ssm, Flag:
    UpTime: 00:01:20
    Upstream interface: GigabitEthernet3/0/0
        Upstream neighbor: 10.110.5.100
        RPF neighbor: 10.110.5.100
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet1/0/0
            Protocol: pim-ssm, UpTime: 00:01:20, Expires:-
<RouterE> display pim routing-table
VPN-Instance: public net
```

```
 Total 1 (*, G) entry; 1 (S, G) entry
 (*, 225.1.1.1)
     RP: 192.168.9.2 (local)
     Protocol: pim-sm, Flag: WC
     UpTime: 00:13:16
     Upstream interface: Register
         Upstream neighbor: 192.168.4.2
         RPF neighbor: 192.168.4.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet3/0/0
             Protocol: pim-sm, UpTime: 00:13:16, Expires: 00:03:22
(10.110.5.100, 227.1.1.1)
     Protocol: pim-ssm, Flag:
     UpTime: 00:01:22
     Upstream interface: GigabitEthernet4/0/0
         Upstream neighbor: 192.168.4.2
         RPF neighbor: 192.168.4.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/0
             Protocol: pim-ssm, UpTime: 00:01:22, Expires:-
<RouterC> display pim routing-table
 VPN-Instance: public net
 Total 1 (S, G) entry
 (10.110.5.100, 227.1.1.1)
     Protocol: pim-ssm, Flag:
     UpTime: 00:01:25
     Upstream interface: GigabitEthernet2/0/0
         Upstream neighbor: 192.168.3.2
         RPF 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:-
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 227.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 192.168.9.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 10.110.1.1 255.255.255.0
 pim sm
 igmp enable
 igmp version 3
 pim silent
#
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 192.168.9.0 0.0.0.255
#
pim
 static-rp 192.168.2.2
 ssm-policy 2000
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 227.1.1.0 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
 static-rp 192.168.2.2
 ssm-policy 2000
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 227.1.1.0 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
 static-rp 192.168.2.2
 ssm-policy 2000
#
return
```

- RouterD 的配置文件

```
#
```

```
 sysname RouterD
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 227.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 192.168.4.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 10.110.5.1 255.255.255.0
 pim sm
#
interface GigabitEthernet4/0/0
 ip address 10.110.4.1 255.255.255.0
 pim sm
 pim bsr-boundary
#
ospf 1
 area 0.0.0.0
  network 10.110.4.0 0.0.0.255
  network 10.110.5.0 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
 ssm-policy 2000
#
return
```

- RouterE 的配置文件

```
#
 sysname RouterE
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 227.1.1.0 0.0.0.255
#
acl number 2005
 rule 5 permit source 225.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 192.168.9.2 255.255.255.0
 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 192.168.3.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 192.168.9.0 0.0.0.255
```

```
  network 192.168.4.0 0.0.0.255
#
pim
 c-bsr GigabitEthernet3/0/0
 c-rp GigabitEthernet3/0/0 group-policy 2005 priority 0
 static-rp 192.168.2.2
 ssm-policy 2000
#
return
```

5.14.2 配置基于 PIM 协议的 Anycast RP 示例

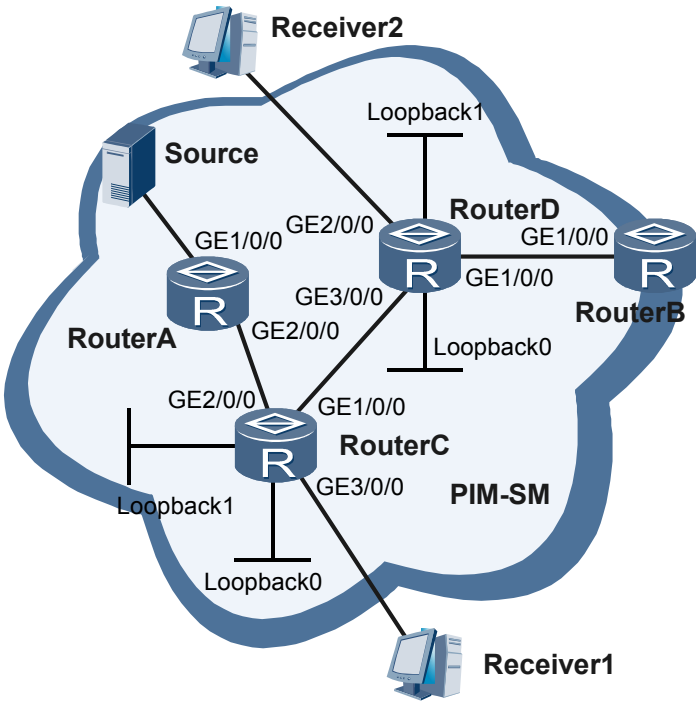
PIM-SM 域内有多个组播源和多个接收者，通过配置 Anycast RP 对等体，可实现组播源就近注册和接收者就近加入，缓解 RP 负担，优化组播数据转发路径。

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 5-3 所示，PIM-SM 域有多个接收者。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 5-3 配置基于 PIM 协议的 Anycast RP 组网图



设备	接口	IP 地址
RouterA	GE 1/0/0	10.110.1.1/24
	GE 2/0/0	192.168.1.1/24
RouterB	GE 1/0/0	192.168.2.1/24

RouterC	GE 1/0/0	192.168.3.1/24
	GE 2/0/0	192.168.1.2/24
	GE 3/0/0	10.110.2.1/24
	Loopback0	1.1.1.1/32
	Loopback1	2.2.2.2/32
RouterD	GE 1/0/0	192.168.2.2/24
	GE 2/0/0	10.110.3.1/24
	GE 3/0/0	192.168.3.2/24
	Loopback0	1.1.1.1/32
	Loopback1	3.3.3.3/32

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。

数据准备

为完成此配置例，需准备如下的数据：

- 组播组地址：226.1.1.1/24
- RP 地址
- Anycast RP 本地地址

操作步骤

步骤 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。使能组播功能，在各接口启动 PIM-SM 功能

按照图 5-3，在 PIM-SM 域内，配置各路由器接口的 IP 地址和掩码，配置各路由器之间采用 OSPF 进行互连。使能组播功能，在各接口启动 PIM-SM 功能。

配置 RouterA。

```
<Huawei> system-view
<Huawei> sysname RouterA
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 10.110.1.1 24
[RouterA-GigabitEthernet1/0/0] pim sm
[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] pim sm
```

```
[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
```

配置 RouterB。

```
<Huawei> system-view
<Huawei> sysname RouterB
[RouterB] multicast routing-enable
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 192.168.2.1 24
[RouterB-GigabitEthernet1/0/0] pim sm
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置 RouterC。

```
<Huawei> system-view
<Huawei> sysname RouterC
[RouterC] multicast routing-enable
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ip address 192.168.3.1 24
[RouterC-GigabitEthernet1/0/0] pim sm
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] ip address 192.168.1.2 24
[RouterC-GigabitEthernet2/0/0] pim sm
[RouterC-GigabitEthernet2/0/0] quit
[RouterC] interface gigabitethernet 3/0/0
[RouterC-GigabitEthernet3/0/0] ip address 10.110.2.1 24
[RouterC-GigabitEthernet3/0/0] pim sm
[RouterC-GigabitEthernet3/0/0] quit
[RouterC] interface loopback 0
[RouterC-LoopBack0] ip address 1.1.1.1 32
[RouterC-LoopBack0] pim sm
[RouterC-LoopBack0] quit
[RouterC] interface loopback 1
[RouterC-LoopBack1] ip address 2.2.2.2 32
[RouterC-LoopBack1] pim sm
[RouterC-LoopBack1] quit
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 192.168.3.0 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 10.110.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

配置 RouterD。

```
<Huawei> system-view
<Huawei> sysname RouterD
[RouterD] multicast routing-enable
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] ip address 192.168.2.2 24
[RouterD-GigabitEthernet1/0/0] pim sm
[RouterD-GigabitEthernet1/0/0] quit
[RouterD] interface gigabitethernet 2/0/0
[RouterD-GigabitEthernet2/0/0] ip address 10.110.3.1 24
[RouterD-GigabitEthernet2/0/0] pim sm
```

```
[RouterD-GigabitEthernet2/0/0] quit
[RouterD] interface gigabitethernet 3/0/0
[RouterD-GigabitEthernet3/0/0] ip address 192.168.3.2 24
[RouterD-GigabitEthernet3/0/0] pim sm
[RouterD-GigabitEthernet3/0/0] quit
[RouterD] interface loopback 0
[RouterD-LoopBack0] ip address 1.1.1.1 32
[RouterD-LoopBack0] pim sm
[RouterD-LoopBack0] quit
[RouterD] interface loopback 1
[RouterD-LoopBack1] ip address 3.3.3.3 32
[RouterD-LoopBack1] pim sm
[RouterD-LoopBack1] quit
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] network 10.110.3.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[RouterD-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[RouterD-ospf-1-area-0.0.0.0] quit
[RouterD-ospf-1] quit
```

步骤 2 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 3 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 4 配置 RouterC 和 RouterD 的 Loopback0 接口为 Anycast RP

配置 RouterC。

```
[RouterC] pim
[RouterC-pim] anycast-rp 1.1.1.1
[RouterC-pim-anycast-rp-1.1.1.1] quit
[RouterC-pim] quit
```

配置 RouterD。

```
[RouterD] pim
[RouterD-pim] anycast-rp 1.1.1.1
[RouterD-pim-anycast-rp-1.1.1.1] quit
```

```
[RouterD-pim] quit
```

步骤 5 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 1.1.1.1
[RouterC-pim-anycast-rp-1.1.1.1] local-address 2.2.2.2
[RouterC-pim-anycast-rp-1.1.1.1] quit
[RouterC-pim] quit
```

配置 RouterD。

```
[RouterD] pim
[RouterC-pim] anycast-rp 1.1.1.1
[RouterC-pim-anycast-rp-1.1.1.1] local-address 3.3.3.3
[RouterC-pim-anycast-rp-1.1.1.1] quit
[RouterD-pim] quit
```

步骤 6 配置 RouterC 和 RouterD 互为 Anycast RP 对等体

配置 RouterC。

```
[RouterC] pim
[RouterC-pim] anycast-rp 1.1.1.1
[RouterC-pim-anycast-rp-1.1.1.1] peer 3.3.3.3
[RouterC-pim-anycast-rp-1.1.1.1] quit
[RouterC-pim] quit
```

配置 RouterD。

```
[RouterD] pim
[RouterD-pim] anycast-rp 1.1.1.1
[RouterD-pim-anycast-rp-1.1.1.1] peer 2.2.2.2
[RouterD-pim-anycast-rp-1.1.1.1] quit
[RouterD-pim] quit
```

步骤 7 检验配置效果

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: 1.1.1.1 (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: 1.1.1.1 (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) entries

 (10.110.1.2, 226.1.1.1)
     RP: 1.1.1.1 (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) entries

 (*, 226.1.1.1)
     RP: 1.1.1.1 (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: 1.1.1.1 (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 1.1.1.1 255.255.255.255
 pim sm
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 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 1.1.1.1 0.0.0.0
  network 2.2.2.2 0.0.0.0
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
 anycast-rp 1.1.1.1
  local-address 2.2.2.2
  peer 3.3.3.3
#
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 1.1.1.1 255.255.255.255
 pim sm
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.0
 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 3.3.3.3 0.0.0.0
  network 1.1.1.1 0.0.0.0
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
 anycast-rp 1.1.1.1
  local-address 3.3.3.3
  peer 2.2.2.2
#
return
```

6 MSDP 配置

关于本章

通过配置 MSDP 协议，可以实现 PIM-SM 域间组播路由与数据转发、PIM-SM 域内的 Anycast RP。

6.1 MSDP 概述
MSDP 的实现方式是在各个 PIM-SM 域的 RP 之间建立 MSDP 对等体关系，MSDP 对等体之间通过交互 SA 消息来传递(S,G)信息，从而共享组播源，主机可以接收其他 PIM-SM 域的组播源数据。

6.2 AR2200-S 支持的 MSDP 特性
系统通过 MSDP 实现 PIM-SM 域间组播和 PIM-SM 域内 Anycast RP。用户可以控制 MSDP 对等体连接，调整 SA 消息参数，配置 MSDP 对等体认证和 SA 消息的过滤策略来提高 MSDP 安全性。系统支持多实例的 MSDP。

6.3 配置 PIM-SM 域内 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，并且在这些 RP 之间建立 MSDP 对等体关系，从而实现组播源就近注册和接收者就近加入。既缓解了单个 RP 的负担，也实现了 RP 备份、优化了转发路径。

6.4 管理 MSDP 对等体连接
MSDP 对等体之间使用 TCP 连接，用户可以断开或重建 TCP 连接来灵活控制 MSDP 对等体间的会话。还可以调整 MSDP 对等体连接的重试周期。

6.5 配置 SA 缓存
SA 缓存用来在本地保存 SA 消息中携带的(S,G)信息，有接收需求时，设备直接从 SA 缓存中获得可用的(S,G)信息。

6.6 配置 SA 请求
远端 MSDP 对等体的 SA Cache 容量较大时，在本地设备上配置“发送 SA 请求消息”可以缩减接收者获取组播源信息的时间。可以在指定的远端 MSDP 对等体上配置接收 SA 请求消息的过滤规则。

6.7 配置过滤 SA 消息的规则
缺省情况下，所有通过 RPF 检查的 SA 消息都会被接收并向其他 MSDP 对等体转发。配置创建、接收或转发 SA 消息的过滤策略可以控制 SA 消息在 MSDP 对等体间的传递。

6.8 配置 MSDP 认证

MSDP 对等体认证包括 MSDP MD5 认证和 Key-Chain 认证，只能选择其中一种认证方式。

6.9 维护 MSDP

MSDP 的维护包括：清除 MSDP 对等体统计信息、清除 SA-Cache 中缓存的(S,G)信息。

6.10 配置举例

通过配置举例，可以了解如何通过 MBGP 对等体实现 PIM-SM 域间组播、通过静态 RPF 对等体实现 AS 间组播、配置 PIM-SM 域内 Anycast RP。

6.1 MSDP 概述

MSDP 的实现方式是在各个 PIM-SM 域的 RP 之间建立 MSDP 对等体关系，MSDP 对等体之间通过交互 SA 消息来传递(S,G)信息，从而共享组播源，主机可以接收其他 PIM-SM 域的组播源数据。

在基本的 PIM-SM 模式下，组播源只向本域内的 RP（Rendezvous Point）注册，且域间组播源信息隔离。因此 RP 知道且仅知道本域内的组播源，只能在本域内建立组播分发树，将本域内的组播源发出的数据分发给本域内的用户。

如果能够加载一种机制，将其它域内的组播源信息传递给本域内的 RP，则本域内的 RP 就可以向其他域内的组播源发起加入过程、建立组播分发树、实现组播数据跨域传输，从而使本域内的组成员主机接收到其他域的组播源发出的数据。

MSDP（Multicast Source Discovery Protocol）是能够解决上述问题的一种机制，成为基于多个 PIM-SM 域互连而开发的一种域间组播解决方案。

MSDP 的实现方式是在各个 PIM-SM 域的 RP 之间建立 MSDP 对等体关系，MSDP 对等体之间通过交互 SA（Source Active）消息，将（S，G）信息从“组播源 S 注册的 RP”传递给其他的“组 G 成员主机加入的 RP”。

MSDP 对等体之间使用 TCP 连接，对接收到的 SA 消息执行 RPF 检查。

说明

MSDP 只适用于 PIM-SM 域，仅对 ASM（Any-Source Multicast）模型有意义。

6.2 AR2200-S 支持的 MSDP 特性

系统通过 MSDP 实现 PIM-SM 域间组播和 PIM-SM 域内 Anycast RP。用户可以控制 MSDP 对等体连接，调整 SA 消息参数，配置 MSDP 对等体认证和 SA 消息的过滤策略来提高 MSDP 安全性。系统支持多实例的 MSDP。

说明

异步串口，ISDN BRI 接口，3G 接口，Bridge-if 接口，NULL 接口，QinQ 子接口不支持 MSDP。

PIM-SM 域内 Anycast RP

在 PIM-SM 域中应用 Anycast RP，可以实现组播源就近注册和接收者就近加入。既缓解了单个 RP 的负担，也实现了 RP 备份、优化了转发路径。

用户可以将 Loopback 接口作为 C-RP 或者静态 RP 的接口、为 SA 消息指定逻辑 RP 地址。

MSDP 对等体连接参数可配置

AR2200-S 提供 MSDP 会话的开启和关闭功能，同时可以配置路由器向远端 MSDP 对等体发出 TCP 连接请求的重试周期。

SA 消息缓存可配置

缺省情况下，路由器上启动了 SA-Cache 功能，可以在本地保存 SA 消息中携带的（S，G）信息。当有接收需求时，路由器直接从 SA-Cache 中获得可用的（S，G）信息。

用户可以配置缓存（S，G）项的最大数量，可以有效的防止 DoS（Deny of Service）攻击。

AR2200-S 允许用户关闭路由器的 SA-Cache 功能。SA-Cache 关闭后，路由器在本地不保存 SA 消息中携带的（S，G）信息。当有接收需求时，必须等待其 MSDP peer 在下一个周期发来的 SA 消息。这将延迟接收者获取组播源信息的时间。

SA 请求可控制

某些路由器不允许在本地启动 SA-Cache 功能或 SA-Cache 的容量设置较小。当有新的接收需求时，路由器无法立即获取有效的（S，G）信息，必须等待其 MSDP peer 在下一个周期发来的 SA 消息。

如果远端 MSDP peer 上启动了 SA-Cache 功能，且 SA-Cache 的容量设置较大，用户可以在本地路由器上配置“发送 SA 请求消息”以缩减接收者获取组播源信息的时间。

同时用户还可以在远端 MSDP Peer 上配置接收 SA 请求消息的过滤规则。

传输突发性组播数据

当某些组播源发送组播数据的时间间隔大于（S，G）表项的超时时间时，一旦有突发性组播数据，源端 DR 只能将组播数据逐个封装在注册报文中，发给源 RP。源 RP 使用 SA 消息将（S，G）信息传输到远端 RP。然后，远端 RP 向组播源的方向发起（S，G）加入，创建 SPT。由于（S，G）表项超时，远端用户将永远无法收到 S 发出的组播数据。

AR2200-S 支持传输突发组播数据功能，用户在源 RP 上启动“在 SA 消息中封装组播数据报文”功能后，源 RP 会将组播数据报文封装在 SA 消息中，发送出去。远端 RP 接收到该 SA 消息后解封装，将组播数据沿 RPT 传输给本域内用户。

同时，配置“TTL 阈值”可以限制封装在 SA 消息中的组播数据报文的传输范围。当 MSDP Peer 接收到封装了组播数据报文的 SA 消息后，检查组播数据报文 IP 头的 TTL 值。如果组播数据报文的 TTL 值小于或等于阈值，则不向特定的远端对等体转发。如果大于阈值，则将组播数据报文 IP 头的 TTL 值减 1，再使用 SA 消息携带组播数据报文发送出去。

SA 消息的创建、接收和转发可控制

缺省情况下，MSDP 路由器接收通过 RPF 检查的所有 SA 消息，并向所有 MSDP 对等体转发。

AR2200-S 允许用户使用以下三种方式配置过滤规则，控制 SA 消息在 MSDP 对等体间的传递。

- 在源端 RP 上配置“创建 SA 消息的组播源过滤规则”。源端 RP 依据此规则过滤本地注册的活动组播源，决定将哪些（S，G）信息发布出去。
- 配置“从远端 MSDP 对等体接收 SA 消息的过滤规则”。当从远端 MSDP 对等体发来的 SA 消息到达路由器时，依据此规则决定是否接收。
- 配置“向远端 MSDP 对等体转发 SA 消息的过滤规则”。在向远端 MSDP 对等体转发 SA 消息之前，依据此规则决定是否转发。

MSDP 认证

配置 MSDP MD5 或 Key-Chain 认证，可以提高 MSDP 对等体之间建立 TCP 连接的安全性。MSDP 对等体两端必须都配置相同的认证密码，才能正常建立 TCP 连接，交互 MSDP 消息。

6.3 配置 PIM-SM 域内 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，并且在这些 RP 之间建立 MSDP 对等体关系，从而实现组播源就近注册和接收者就近加入。既缓解了单个 RP 的负担，也实现了 RP 备份、优化了转发路径。

6.3.1 建立配置任务

在 PIM-SM 域内各设备单播互通，使能了组播路由且各接口使能了 PIM-SM，网络中未配置 RP 的情况下配置 Anycast RP。

应用环境

在传统的 PIM-SM 域中，每个组播组都只能映射到一个 RP。当网络负载较大或者流量过于集中时，可能导致 RP 路由器的压力过大，RP 失效后收敛较慢，组播转发路径非最优等问题。

在 PIM-SM 域中应用 Anycast RP，可以实现组播源就近注册和接收者就近加入。既缓解了单个 RP 的负担，也实现了 RP 备份、优化了转发路径。

推荐的配置方案如下。

- 在 PIM-SM 域中的多台路由器上，各准备一个 Loopback 接口，配置相同的 IP 地址，并使用单播路由发布出去。
- 在这些路由器上配置该 Loopback 接口为 C-RP，或在 PIM-SM 域中的所有路由器上配置该地址为静态 RP。
- 在这些路由器之间建立 MSDP 对等体。如果这些路由器的总数超过三个，建议两两之间建立 MSDP 对等体关系并加入同一个 Mesh Group。
- 为在这些 MSDP 对等体之间传递的 SA 消息指定逻辑 RP 地址。

前置任务

在配置 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
- 使能 IP 组播
- 配置 PIM-SM 域，未配置 RP

数据准备

在配置 Anycast RP 之前，需准备以下数据。

序号	数据
1	RP 地址

序号	数据
2	本端 MSDP 对等体的接口、地址
3	远端 MSDP 对等体的接口、地址
4	MSDP 对等体描述信息

6.3.2 配置 RP 接口地址

在 PIM-SM 域内有待建立 Anycast RP 的多台设备上，各准备一个 Loopback 接口，配置相同的 IP 地址。使用单播路由将 RP 接口地址发布出去，确保网络各个位置的设备都有到达该 RP 接口地址的路由。

背景信息

使用当前网络中的单播路由协议，将新配置的 RP 接口地址公布出去。确保网络各个位置的路由器上都有到达该 RP 地址的路由。

在 PIM-SM 域内有待建立 Anycast-RP 的多台路由器上，分别进行如下配置。

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 loopback** *interface-number*，进入 Loopback 接口视图。

由于网络中将同时存在多个 RP 使用相同的 IP 地址，所以选择将 RP 配置在 Loopback 接口上。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置 Loopback 接口地址。

- *ip-address*：RP 的地址。在多台设备上配置 RP 接口，使用相同的 IP 地址。
- *mask* | *mask-length*：Loopback 接口地址掩码。

步骤 4 执行命令 **pim sm**，为 RP 接口使能 PIM-SM。

说明

配置动态 RP 前需要在接口上使能此命令。若配置静态 RP，不需要使能此命令。

----结束

6.3.3 配置 C-RP

若选择 C-RP，则只在有待建立 Anycast RP 的设备上将 Loopback 接口配置为候选 RP 接口。

背景信息

说明

- 当 PIM-SM 网络使用静态 RP 时，跳过此项配置。
- 当 PIM-SM 网络使用 BSR-RP 时，必须执行此项配置。执行此项配置之前，需要先配置 BSR 和 BSR 边界，且 BSR 的地址不能与该 C-RP 地址相同。

在 PIM-SM 域内有待建立 Anycast-RP 的多台路由器上，分别进行如下配置。

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** ，进入 PIM 视图。

步骤 3 执行命令 **c-rp loopback** *interface-number*，指定该 Loopback 接口为候选 RP 接口。

----结束

6.3.4 配置静态 RP

若使用静态 RP，则需要在 PIM-SM 域内的所有设备上将 Loopback 接口地址配置为 RP。

背景信息

说明

- 当 PIM-SM 网络使用 BSR-RP 时，跳过此项配置。
- 当 PIM-SM 网络使用静态 RP 时，必须执行此项配置。

在本 PIM-SM 域内所有路由器上，分别进行如下配置。

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** ，进入 PIM 视图。

步骤 3 执行命令 **static-rp** *rp-address*，配置静态 RP 的地址为 Loopback 接口地址。

----结束

6.3.5 配置 MSDP 对等体

在 RP 之间建立 MSDP 对等体。如果这些设备的总数超过三个，建议两两之间建立 MSDP 对等体关系并加入同一个 Mesh Group。

背景信息

在有待建立 Anycast-RP 的多台路由器上，分别进行如下配置。

说明

如果配置了相同 IP 地址的 RP 的路由器不只两台，确保这些路由器之间使用 MSDP 对等体连通。

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 **msdp** ，启动公网实例的 MSDP 功能，并进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **connect-interface** *interface-type interface-number*，创建 MSDP 对等体连接。

- *peer-address*：远端 MSDP 对等体地址。
- *interface-type interface-number*：本地接口。

步骤 4 （可选）执行命令 **peer** *peer-address* **description** *text*，为 MSDP 对等体添加描述信息。

此项配置有助于区分远端 MSDP 对等体，管理与远端 MSDP 对等体之间的连接。

- *peer-address*：远端 MSDP 对等体的地址。
- *text*：描述性文本，最长为 80 个字符。

步骤 5 （可选）执行命令 **peer** *peer-address* **mesh-group** *name*，配置远端 MSDP 对等体加入 Mesh Group，即承认远端 MSDP 对等体为 Mesh Group 成员。

如果建立 Anycast-RP 的路由器只有两个，则不必执行此项配置。

- *peer-address*：远端 MSDP 对等体地址。
- *name*：Mesh Group 的名称。同一 Mesh group 的组成员使用相同的 Mesh Group 名称。

配置注意事项：

- Mesh Group 所有成员之间必须两两建立 MSDP 对等体连接。
- Mesh Group 所有成员之间必须两两承认对方为 Mesh Group 成员。
- 一个 MSDP 对等体只能属于一个 Mesh Group。如果多次配置同一 MSDP Peer 加入不同的 Mesh Group，最后一个配置有效。

----结束

6.3.6 为 SA 消息指定逻辑 RP 地址

MSDP 对等体对接收到的 SA 消息进行 RPF 检查，如果发现 SA 消息中携带的对端 RP 地址与本地 RP 地址相同，将会丢弃该 SA 消息。所以，需要在有待建立 Anycast RP 的设备上为 SA 消息指定逻辑 RP 地址。

背景信息

MSDP 对等体对接收到的 SA 消息进行 RPF 检查。如果发现 SA 消息中携带的对端 RP 地址与本地 RP 地址相同，将会丢弃该 SA 消息。

在有待建立 Anycast-RP 的多台路由器上，分别进行如下配置。

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 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **originating-rp** *interface-type interface-number*，配置逻辑 RP 接口，不能与实际 RP 接口相同。建议配置为 MSDP 对等体接口。

使用 **originating-rp** 命令后，路由器发出的 SA 消息将携带逻辑 RP 地址，取代 SA 消息报文头中的 RP 地址，到达对端后能够通过 RPF 检查。

说明

系统不向私网发布 MTI 接口上的路由，因此不要将 MTI 接口的地址作为“逻辑 RP”。

----结束

6.3.7 检查配置结果

配置 PIM-SM 域内 Anycast RP 成功后，可以通过命令查看 MSDP 对等体的概要信息和 PIM 路由表项对应的 RP 信息。

操作步骤

- 使用 **display msdp brief** 命令查看 MSDP 对等体状态的简要信息。
- 使用 **display pim routing-table** 命令查看 PIM 路由表项对应的 RP 信息。

----结束

任务示例

在各个 RP 上执行命令 **display msdp brief**，查看远端 MSDP Peer 的简要状态信息。例如：

```
<Huawei> display msdp brief
MSDP Peer Brief Information
  Configured    Up           Listen       Connect      Shutdown     Down
  1             1            0            0            0            0

  Peer's Address     State     Up/Down time    AS     SA Count    Reset Count
  2.2.2.2              UP        00:10:17      ?        0           0
```

在各个 RP 上执行命令 **display pim routing-table**，查看路由表项对应的 RP 信息。

```
<Huawei> display pim routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry
(10.11.1.2, 225.1.1.1)
     RP: 7.7.7.7 (local)
     Protocol: pim-sm, Flag: SPT ACT
     UpTime: 00:01:57
     Upstream interface: GigabitEthernet2/0/0
         Upstream neighbor: 10.3.1.2
         RPF prime neighbor: 10.3.1.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/0
             Protocol: pim-sm, UpTime:  - , Expires:  -
```

6.4 管理 MSDP 对等体连接

MSDP 对等体之间使用 TCP 连接，用户可以断开或重建 TCP 连接来灵活控制 MSDP 对等体间的会话。还可以调整 MSDP 对等体连接的重试周期。

6.4.1 建立配置任务

配置 PIM-SM 域间组播或 PIM-SM 域内 Anycast RP 后，可以根据实际需要管理 MSDP 对等体连接。

应用环境

MSDP 对等体之间使用 TCP 连接（端口 639）。用户可以断开或重建 TCP 连接，灵活**控制 MSDP 对等体之间的会话**。

当新创建了 MSDP 对等体、或重新启动某被关闭的 MSDP 对等体连接、或故障的 MSDP 对等体尝试恢复工作时，需要迅速在 MSDP 对等体之间建立 TCP 连接。用户可以灵活的**调整 MSDP 对等体连接的重试周期**。

前置任务

在配置管理 MSDP 对等体连接之前，需完成以下任务：

- 配置单播路由协议，实现网络层互通
- 使能 IP 组播
- 配置 PIM-SM 域，实现域内组播
- **配置 PIM-SM 域内 Anycast RP**

数据准备

在配置管理 MSDP 对等体连接之前，需准备以下数据。

序号	数据
1	远端 MSDP 对等体地址
2	本端路由器向远端 MSDP 对等体发出 TCP 连接请求的重试周期

6.4.2 控制 MSDP 对等体之间的会话

在创建了 MSDP 对等体的设备上关闭 MSDP 对等体连接，对等体之间不再传递 SA 消息，并不再重试建立连接。用户可以根据需要重新启动 MSDP 对等体连接。

背景信息

在创建了 MSDP 对等体的路由器上进行如下配置。

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 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **shutdown** *peer-address*，关闭与远端 MSDP 对等体之间的会话。

- *peer-address* 为远端 MSDP 对等体地址。
- 关闭与远端 MSDP 对等体之间的会话后，TCP 连接断开，对等体之间不再传递 SA 消息，并不再重试建立连接，但配置信息会保留。
- 执行命令 **undo shutdown** *peer-address*，可以打开与远端 MSDP 对等体之间会话，重新建立 TCP 连接。

----结束

6.4.3 调整 MSDP 对等体连接的重试周期

当新创建了 MSDP 对等体、重新启动被关闭的 MSDP 对等体连接、或故障的 MSDP 对等体尝试恢复工作时，需要迅速在 MSDP 对等体之间建立 TCP 连接。用户可以灵活的调整 MSDP 对等体连接的重试周期。

背景信息

在创建了 MSDP 对等体的路由器上进行如下配置。

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 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **timer retry** *interval*，配置路由器向远端 MSDP 对等体发出 TCP 连接请求的重试周期。

----结束

6.4.4 检查配置结果

管理 MSDP 对等体连接后，可以通过命令查看 MSDP 对等体的概要信息和详细信息。

操作步骤

- 使用 **display msdp brief** 命令查看 MSDP 对等体状态的简要信息。
- 使用 **display msdp peer-status** [*peer-address*]命令查看 MSDP 对等体状态的详细信息。

----结束

任务示例

执行命令 **display msdp brief**，查看与远端 MSDP 对等体之间的连接状态简要信息。例如：

```
<Huawei> display msdp brief
MSDP Peer Brief Information
  Configured   Up           Listen       Connect      Shutdown     Down
  2            2            0            0            0            0

  Peer's Address     State     Up/Down time     AS     SA Count    Reset Count
  192.168.2.1           UP        01:07:08     200        8           0
  192.168.4.2           UP        00:06:39     100        13          0
```

6.5 配置 SA 缓存

SA 缓存用来在本地保存 SA 消息中携带的(S,G)信息，有接收需求时，设备直接从 SA 缓存中获得可用的(S,G)信息。

6.5.1 建立配置任务

配置 PIM-SM 域间组播或 PIM-SM 域内 Anycast RP 后，可以根据实际需要配置 SA 缓存。

应用环境

缺省情况下，配置了 MSDP Peer 的路由器上启动了 SA-Cache 功能，可以在本地保存 SA 消息中携带的（S，G）信息。当有接收需求时，路由器直接从 SA-Cache 中获得可用的（S，G）信息。

同时配置缓存（S，G）项的最大数量，可以有效的防止 DoS（Deny of Service）攻击。

AR2200-S 允许用户关闭路由器的 SA-Cache 功能。SA-Cache 关闭后，路由器在本地不保存 SA 消息中携带的（S，G）信息。当有接收需求时，必须等待其 MSDP peer 在下一个周期发来的 SA 消息。这将延迟接收者获取组播信息的时间。

前置任务

在配置 SA 缓存之前，需完成以下任务：

- 配置某单播路由协议，实现网络层互通
- 使能 IP 组播
- 配置 PIM-SM 域，实现域内组播
- **配置 PIM-SM 域内 Anycast RP**

数据准备

在配置 SA 缓存之前，需准备以下数据。

序号	数据
1	SA 缓存的（S, G）项最大数量

6.5.2 配置缓存（S，G）项的最大数量

配置 SA 缓存(S,G)表项的最大数量可以防止 DoS 攻击。

背景信息

在配置了 MSDP Peer 的路由器上，进行如下的配置。

说明

当不进行此项配置时，使用系统缺省值。

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 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **sa-cache-maximum** *sa-limit*，限制被缓存的（S，G）项的最大数量。

- *peer-address* 为远端 MSDP Peer 地址。
- *sa-limit* 为缓存（S，G）项的最大数量。配置值小于 cache 规格时按配置值生效，配置值大于 cache 规格时按规格生效。

----结束

6.5.3 关闭 SA-Cache 功能

系统允许用户关闭 SA Cache 功能。有接收需求时，必须等待其 MSDP 对等体在下一个周期发来的 SA 消息，这将延迟接收者获取组播信息的时间。

背景信息

在配置了 MSDP Peer 的路由器上，进行如下的配置。

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 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **undo cache-sa-enable**，关闭 SA-Cache 功能。

说明

在 MSDP 视图下执行命令 **cache-sa-enable**，可以重新启动 SA-Cache 功能。

----结束

6.5.4 检查配置结果

配置 SA 缓存成功后，可以通过命令查看 SA 缓存中的表项相关信息。

操作步骤

- 使用 **display msdp sa-cache** [*group-address* | *source-address* | [*2-byte-as-number* | *4-byte-as-number*]] *命令查看公网实例的 SA 缓存中的（S，G）项。
- 使用 **display msdp sa-count** [*2-byte-as-number* | *4-byte-as-number*]命令查看公网实例的 SA 缓存中的（S，G）项的数量。

----结束

任务示例

执行命令 **display msdp sa-cache**，查看 SA 缓存中的（S，G）信息。

```
<Huawei> display msdp sa-cache
MSDP Source-Active Cache Information
MSDP Total Source-Active Cache - 3 entries
MSDP matched 3 entries

(8.8.8.8, 225.0.0.200)
 Origin RP: 4.4.4.4
 Pro: BGP, AS: 10
 Uptime: 00:00:33, Expires: 00:05:27

(8.8.8.8, 225.0.0.201)
 Origin RP: 4.4.4.4
 Pro: BGP, AS: 1.0
 Uptime: 00:00:33, Expires: 00:05:27

(8.8.8.8, 225.0.0.202)
 Origin RP: 4.4.4.4
 Pro: BGP, AS: 65535.65535
 Uptime: 00:00:33, Expires: 00:05:27
```

执行命令 **display msdp sa-count**，查看 SA 缓存中的（S，G）项的数量。

```
<Huawei> display msdp sa-count
MSDP Source-Active Count Information
Number of cached Source-Active entries, counted by Peer
  Peer's Address     Number of SA
  10.10.10.10        5
Number of source and group, counted by AS
  AS     Number of source    Number of group
  ?      3                   3
  Total 5 Source-Active entries matched
```

6.6 配置 SA 请求

远端 MSDP 对等体的 SA Cache 容量较大时，在本地设备上配置“发送 SA 请求消息”可以缩减接收者获取组播源信息的时间。可以在指定的远端 MSDP 对等体上配置接收 SA 请求消息的过滤规则。

6.6.1 建立配置任务

配置 PIM-SM 域间组播或 PIM-SM 域内 Anycast RP 后，可以根据实际需要配置 SA 请求。

应用环境

某些路由器 SA-Cache 的容量设置较小。当有新的接收需求时，路由器无法立即获取有效的（S，G）信息，必须等待其 MSDP peer 在下一个周期发来的 SA 消息。

如果远端 MSDP peer 上启动了 SA-Cache 功能，且 SA-Cache 的容量设置较大，则在本地路由器上配置“发送 SA 请求消息”可以缩减接收者获取组播源信息的时间。

- 当本地路由器上有新的接收需求时，主动向某指定远端 MSDP peer 发送 SA 请求消息。
- 远端 MSDP peer 一旦接收到 SA 请求消息，立即回复 SA 消息，携带符合需求的（S，G）信息。如果远端 MSDP peer 上配置了“SA 请求消息过滤规则”，则对从指定对等体发来的 SA 请求消息执行检查，根据检查结果决定是否给予回复。

前置任务

在配置“SA 请求”之前，需完成以下任务：

- 配置某单播路由协议，实现网络层互通
- 使能 IP 组播
- 配置 PIM-SM 域，实现域内组播
- **配置 PIM-SM 域内 Anycast RP**

数据准备

在配置“SA 请求”之前，需准备以下数据。

序号	数据
1	远端 MSDP peer 地址
2	接收 SA 请求消息的过滤列表

6.6.2 在本地路由器上配置“发送 SA 请求消息”

当设备接收到一个新的组加入消息，并且本地表项和 SA 缓存中都没有该(S,G)时，设备可以立即向指定的 MSDP 对等体发送 SA 请求消息，而不是等待下一周期 SA 消息的到来。

背景信息

在本地路由器上，进行如下的配置。

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 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **request-sa-enable**，配置“发送 SA 请求消息”。

peer-address 为远端 MSDP 对等体地址。当本地路由器接收到一个新的组加入消息时，只向 *peer-address* 发送 SA 请求消息。

----结束

6.6.3 （可选）在远端 MSDP peer 上配置接收 SA 请求消息的过滤规则

可以在指定的远端 MSDP 对等体上配置本地设备发出的 SA 请求消息的过滤策略。若 SA 请求消息通过过滤，立即回复 SA 消息。

背景信息

在命令 **peer** *peer-address* **request-sa-enable** 中指定远端 MSDP Peer 的路由器上，进行如下的配置。当不进行此项配置时，一旦有 SA 请求消息到达，路由器立即回复 SA 消息，携带符合需求的（S，G）信息。

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 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **sa-request-policy** [**acl** { *basic-acl-number* | *acl-name* }]，配置接收 SA 请求消息的过滤规则。

- *peer-address* 为发出 SA 请求消息的 MSDP 对等体地址。
- **acl** 为过滤策略。如果没有指定 ACL 则忽略从该 peer 发来的所有 SA 请求；如果指定了 ACL 则仅接收符合规则的 SA 请求消息，其它的被忽略。

----结束

6.6.4 检查配置结果

配置 SA 请求成功后，可以通过命令查看 MSDP 对等体的详细信息和 SA 缓存信息。

操作步骤

- 使用 **display msdp peer-status** [*peer-address*]命令查看 MSDP 对等体状态的详细信息。
- 使用 **display msdp sa-cache** [*group-address* | *source-address* | [*2-byte-as-number* | *4-byte-as-number*]] *命令查看公网实例的 SA 缓存信息。

----结束

任务示例

执行命令 **display msdp peer-status** [*peer-address*]，查看 Information about SA-Requests 字段检查本节配置是否生效。例如：

```
<Huawei> display msdp peer-status
  MSDP Peer 172.40.41.1, AS ?
  Description:
  Information about connection status:
    State: Up
    Up/down time: 00:26:41
    Resets: 0
    Connection interface: GigabitEthernet2/0/0 (172.40.41.2)
    Number of sent/received messages: 27/28
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 00:26:56
  Information about (Source, Group)-based SA filtering policy:
    Import policy: none
    Export policy: none
  Information about SA-Requests:
    Policy to accept SA-Request messages: 2000
    Sending SA-Requests status: enable
  Minimum TTL to forward SA with encapsulated data: 0
  SAs learned from this peer: 0, SA-cache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 16/0
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
    Incoming/outgoing data packets: 0/0
    Peer authentication: configured
    Peer authentication type: Key-Chain
```

6.7 配置过滤 SA 消息的规则

缺省情况下，所有通过 RPF 检查的 SA 消息都会被接收并向其他 MSDP 对等体转发。配置创建、接收或转发 SA 消息的过滤策略可以控制 SA 消息在 MSDP 对等体间的传递。

6.7.1 建立配置任务

配置 PIM-SM 域间组播或 PIM-SM 域内 Anycast RP 后，可以根据实际需要配置 SA 消息的过滤规则。

应用环境

缺省情况下，MSDP 的路由器接收通过 RPF 检查的所有 SA 消息，并向所有 MSDP 对等体转发。AR2200-S 允许用户使用以下三种方式配置过滤规则，控制 SA 消息在 MSDP 对等体间的传递。

- 在源端 RP 上配置“创建 SA 消息的组播源过滤规则”。源端 RP 依据此规则过滤本地注册的活动组播源，决定将哪些（S，G）信息发布出去。
- 配置“从远端 MSDP 对等体接收 SA 消息的过滤规则”。当从远端 MSDP 对等体发来的 SA 消息到达路由器时，依据此规则决定是否接收。
- 配置“向远端 MSDP 对等体转发 SA 消息的过滤规则”。在向远端 MSDP 对等体转发 SA 消息之前，依据此规则决定是否转发。

前置任务

在配置“控制 SA 消息的创建与转发”之前，需完成以下任务：

- 配置某单播路由协议，实现网络层互通
- 使能 IP 组播
- 配置 PIM-SM 域，实现域内组播
- **配置 PIM-SM 域内 Anycast RP**

数据准备

在配置“控制 SA 消息的创建与转发”之前，需准备以下数据。

序号	数据
1	创建 SA 消息的过滤列表
2	接收 SA 消息的过滤列表
3	转发 SA 消息的过滤列表
4	远端 MSDP peer 地址

6.7.2 配置创建 SA 消息的规则

在源端 RP 上配置“创建 SA 消息的组播源过滤规则”。源端 RP 依据此规则过滤本地注册的活动组播源，决定将哪些(S,G)信息发布出去。

背景信息

在配置了 MSDP Peer 的源 RP 上，进行如下的配置。

说明

当不进行此项配置时，源 RP 创建的 SA 消息中包含所有本地活动源信息。

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 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **import-source** [**acl** { *acl-number* | *acl-name* }]，配置创建 SA 消息的组播源过滤规则。

- **acl** 为组播源过滤列表。MSDP 创建 SA 消息时只包含符合指定过滤规则的本地源信息，从而可以控制本地（S，G）信息的外流。
- 如果执行不带 **acl** 参数的 **import-source** 命令，SA 消息将不通告任何本地活动源信息。

----结束

6.7.3 配置接收 SA 消息的规则

在远端 MSDP 对等体上配置“接收 SA 消息的过滤规则”。当从远端 MSDP 对等体发来的 SA 消息到达设备时，依据此规则决定是否接收。

背景信息

在配置了 MSDP Peer 的路由器上，进行如下的配置。

说明

当不进行此项配置时，路由器接收所有通过 RPF 检查的 SA 消息。

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 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **sa-policy import** [**acl** { *advanced-acl-number* | *acl-name* }]，配置从远端 MSDP 对等体接收 SA 消息的过滤规则。

- *peer-address* 为远端 MSDP 对等体地址。
- **acl** 指定高级过滤列表。在来自 *peer-address* 的 SA 消息中，选择接收通过该 ACL 规则过滤的（S，G）信息。
- 如果执行不带 **acl** 参数的 **peer** *peer-address* **sa-policy import** 命令，则路由器不接收来自 *peer-address* 的任何（S，G）信息。

----结束

6.7.4 配置转发 SA 消息的规则

在本地设备上配置“向远端 MSDP 对等体转发 SA 消息的过滤规则”。在向远端 MSDP 对等体转发 SA 消息之前，依据此规则决定是否转发。

背景信息

在配置了 MSDP Peer 的路由器上，进行如下的配置。

说明

当不进行此项配置时，路由器转发所有通过 RPF 检查的 SA 消息。

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 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **sa-policy export** [**acl** { *advanced-acl-number* | *acl-name* }]，配置向远端 MSDP 对等体转发 SA 消息的过滤规则。

- *peer-address* 为远端 MSDP 对等体地址。
- **acl** 指定高级过滤列表。只有通过该 ACL 规则过滤的（S，G）信息才向 *peer-address* 转发。
- 如果执行不带 **acl** 参数的 **peer** *peer-address* **sa-policy export** 命令，则路由器不向 *peer-address* 转发任何（S，G）信息。

----结束

6.7.5 检查配置结果

配置过滤 SA 消息的规则成功后，可以通过命令查看 MSDP 对等体的详细信息和 SA 缓存信息。

操作步骤

- 使用 **display msdp sa-cache** [*group-address* | *source-address* | [*2-byte-as-number* | *4-byte-as-number*]] *命令查看公网实例的 SA 缓存信息。
- 使用 **display msdp peer-status** [*peer-address*]命令查看 MSDP 对等体状态的详细信息。

----结束

任务示例

执行命令 **display msdp peer-status** [*peer-address*]，查看 Information about (Source, Group)-based SA filtering policy 字段，检查本节配置是否生效。例如：

```
<Huawei> display msdp peer-status
  MSDP Peer 172.40.41.1, AS ?
  Description:
  Information about connection status:
    State: Up
    Up/down time: 00:26:41
    Resets: 0
    Connection interface: GigabitEthernet2/0/0 (172.40.41.2)
    Number of sent/received messages: 27/28
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 00:26:56
  Information about (Source, Group)-based SA filtering policy:
    Import policy: 3000
    Export policy: 3002
  Information about SA-Requests:
    Policy to accept SA-Request messages: 2000
    Sending SA-Requests status: enable
  Minimum TTL to forward SA with encapsulated data: 10
  SAs learned from this peer: 0, SA-cache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 16/0
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
    Incoming/outgoing data packets: 0/0
    Peer authentication: unconfigured ,
    Peer authentication type: none
```

执行命令 **display msdp sa-cache**，查看 SA 缓存中的（S，G）信息。

- 如果指定了 *group-address*，则显示指定组对应的（S，G）表项。

- 如果指定了 *source-address*，则显示指定源对应的（S，G）表项。
- 如果指定了 *2-byte-as-number* 或 *4-byte-as-number*，则显示源 RP 属于指定 AS 的（S，G）表项。

```
<Huawei> display msdp sa-cache
MSDP Source-Active Cache Information
MSDP Total Source-Active Cache - 3 entries
MSDP matched 3 entries

(8.8.8.8, 225.0.0.200)
 Origin RP: 4.4.4.4
 Pro: BGP, AS: 10
 Uptime: 00:00:33, Expires: 00:05:27

(8.8.8.8, 225.0.0.201)
 Origin RP: 4.4.4.4
 Pro: BGP, AS: 1.0
 Uptime: 00:00:33, Expires: 00:05:27

(8.8.8.8, 225.0.0.202)
 Origin RP: 4.4.4.4
 Pro: BGP, AS: 65535.65535
 Uptime: 00:00:33, Expires: 00:05:27
```

6.8 配置 MSDP 认证

MSDP 对等体认证包括 MSDP MD5 认证和 Key-Chain 认证，只能选择其中一种认证方式。

6.8.1 建立配置任务

配置 PIM-SM 域间组播或 PIM-SM 域内 Anycast RP 后，可以根据实际需要配置 MSDP 认证来提高 MSDP 对等体之间建立 TCP 连接的安全性。

应用环境

配置认证可以提高 MSDP 对等体之间建立 TCP 连接的安全性。

前置任务

在配置 MSDP 认证之前，需完成以下任务：

- 配置某单播路由协议，实现网络层互通
- 使能 IP 组播
- 配置 PIM-SM 域，实现域内组播
- **配置 PIM-SM 域内 Anycast RP**

数据准备

在配置 MSDP 认证之前，需要准备以下数据。

序号	数据
1	需要配置 MSDP 认证的对等体地址
2	MSDP MD5 认证的密码

序号	数据
3	MSDP Key-Chain 认证的 Key-Chain 名称

6.8.2 配置 MSDP MD5 认证

MSDP 对等体两端必须都配置相同的认证密码，才能正常建立 TCP 连接，交互 MSDP 消息。可以一端为明文形式，一端为密文形式。

背景信息

缺省情况下，没有配置 MSDP MD5 认证。

在配置了 MSDP 对等体的路由器上，进行如下的配置。

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 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **password** { **cipher** *cipher-password* | **simple** *simple-password* }，配置 MSDP MD5 认证。

密码不支持空格，区分大小写。

MSDP 对等体两端必须都配置相同的认证密码，才能正常建立 TCP 连接，交互 MSDP 消息。可以一端为明文形式，一端为密文形式。

说明

MSDP MD5 认证与 MSDP Key-Chain 认证互斥。

符号^#^#和$@$@用来识别变长密码，^#^#作为新密码的前缀和后缀，$@$@作为老密码的前缀和后缀，所以不支持以“$@$@”或“^#^#”同时作为明文密码的起始和结束字符。

----结束

6.8.3 配置 MSDP Key-Chain 认证

MSDP 对等体两端必须都配置 Key-Chain 认证，且配置的 Key-Chain 必须使用相同的加密算法和密码，才能正常建立 TCP 连接，交互 MSDP 消息。

背景信息

缺省情况下，没有配置 MSDP Key-Chain 认证。

在配置了 MSDP 对等体的路由器上，进行如下的配置。

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 **msdp** ，进入 MSDP 视图。

步骤 3 执行命令 **peer** *peer-address* **keychain** *keychain-name*，配置 MSDP Key-Chain 认证。

MSDP 对等体两端必须都配置 Key-Chain 认证，且配置的 Key-Chain 必须使用相同的加密算法和密码，才能正常建立 TCP 连接，交互 MSDP 消息。

配置 MSDP Key-Chain 认证前，必须配置 *keychain-name* 对应的 Key-Chain，否则 TCP 连接不能正常建立。

说明

MSDP MD5 认证与 MSDP Key-Chain 认证互斥。

----结束

6.8.4 检查配置结果

配置 MSDP 认证成功后，可以通过命令查看 MSDP 对等体的简要信息和详细信息。

操作步骤

- 使用 **display msdp brief** 命令查看 MSDP 对等体状态的简要信息。
- 使用 **display msdp peer-status** [*peer-address*]命令查看 MSDP 对等体状态的详细信息。

----结束

任务示例

执行命令 **display msdp peer-status** [*peer-address*]，查看 Peer authentication 和 Peer authentication type 字段，检查本节配置是否生效。例如：

```
<Huawei> display msdp peer-status
  MSDP Peer 172.40.41.1, AS ?
  Description:
  Information about connection status:
    State: Up
    Up/down time: 00:26:41
    Resets: 0
    Connection interface: GigabitEthernet2/0/0 (172.40.41.2)
    Number of sent/received messages: 27/28
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 00:26:56
  Information about (Source, Group)-based SA filtering policy:
    Import policy: 3000
    Export policy: 3002
  Information about SA-Requests:
    Policy to accept SA-Request messages: 2000
    Sending SA-Requests status: enable
  Minimum TTL to forward SA with encapsulated data: 10
  SAs learned from this peer: 0, SA-cache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 16/0
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
    Incoming/outgoing data packets: 0/0
    Peer authentication: configured
    Peer authentication type: Key-Chain
```

6.9 维护 MSDP

MSDP 的维护包括：清除 MSDP 对等体统计信息、清除 SA-Cache 中缓存的(S,G)信息。

6.9.1 清除 MSDP 对等体统计信息

清除 MSDP 对等体的统计信息时，可根据实际情况选择重置或不重置 MSDP 对等体之间的 TCP 连接，注意清除后无法恢复。重置 TCP 连接会影响 MSDP 的运行。

背景信息

注意

清除 MSDP 对等体统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

- 在确认需要重置与指定 MSDP 对等体的 TCP 连接，并清除指定 MSDP 对等体的所有统计信息后，请在用户视图下执行 **reset msdp peer** [*peer-address*]命令。
- 在确认需要在不重置 MSDP 对等体的情况下清除一个或多个 MSDP 对等体的统计信息后，请在用户视图下执行 **reset msdp statistics** [*peer-address*]命令。
- 在确认需要清除接收、发送和丢弃的 MSDP 报文的计数后，请在用户视图下执行 **reset msdp control-message counters** [**peer** *peer-address*]命令。

----结束

6.9.2 清除 SA-Cache 中缓存的（S，G）信息

需要重置 SA Cache 中的内容时，可以清除 SA Cache 中缓存的所有(S,G)信息，注意清除后无法恢复。

背景信息

注意

清除 SA-Cache 中缓存的（S，G）信息后，以前的（S，G）信息将无法恢复，务必仔细确认。

操作步骤

步骤 1 在确认需要清除 SA-Cache 中缓存的（S，G）信息后，请在用户视图下执行 **reset msdp sa-cache** [*group-address*]命令。

----结束

6.10 配置举例

通过配置举例，可以了解如何通过 MBGP 对等体实现 PIM-SM 域间组播、通过静态 RPF 对等体实现 AS 间组播、配置 PIM-SM 域内 Anycast RP。

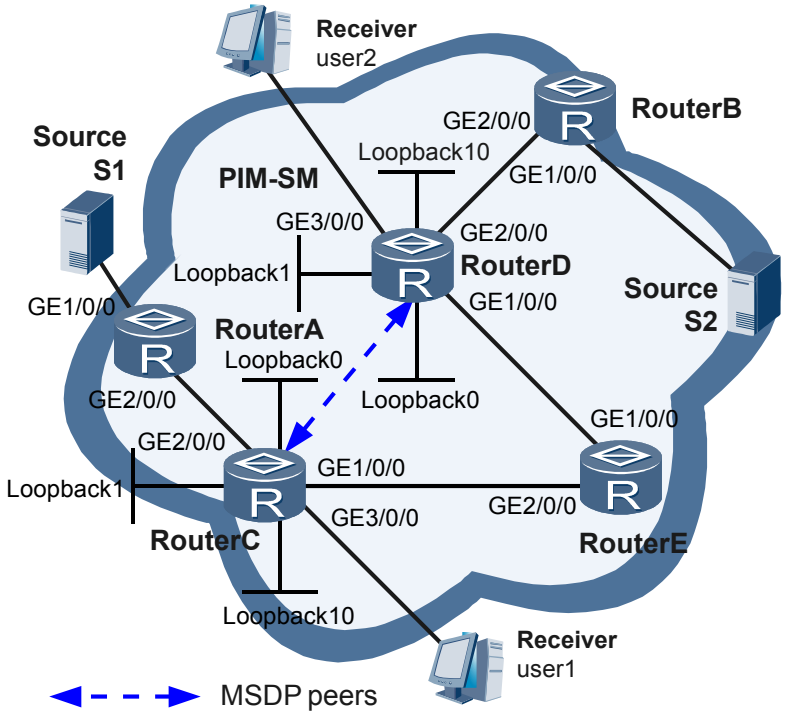
6.10.1 配置 Anycast RP 示例

PIM-SM 域内有多个组播源和多个接收者，在多个 C-RP 间配置 MSDP 对等体，通过 Anycast RP 实现 RP 负荷分担。

组网需求

如图 6-1 所示，PIM-SM 域拥有多个组播源和多个接收者。需求：在 PIM-SM 域内建立 MSDP 对等体实现 RP 负荷分担。

图 6-1 配置 Anncast RP 组网图



Device	接口	IP 地址	Device	接口	IP 地址
RouterA	GE1/0/0	10.110.5.1/24	RouterD	GE1/0/0	192.168.3.1/24
	GE2/0/0	10.110.1.2/24		GE2/0/0	10.110.2.1/24
RouterB	GE1/0/0	10.110.6.1/24		GE3/0/0	10.110.3.1/24
	GE2/0/0	10.110.2.2/24		Loopback0	2.2.2.2/32
RouterC	GE1/0/0	192.168.1.1/24		Loopback1	4.4.4.4/32
	GE2/0/0	10.110.1.1/24		Loopback10	10.1.1.1/32
	GE3/0/0	10.110.4.1/24	RouterE	GE1/0/0	192.168.3.2/24
	Loopback0	1.1.1.1/32		GE2/0/0	192.168.1.2/24
	Loopback1	3.3.3.3/32			
	Loopback10	10.1.1.1/32			

配置思路

设计方案：配置 Anycast RP，接收者向拓扑距离最近的 RP 发起加入，组播源向拓扑距离最近的 RP 发起注册。步骤如下：

1. 配置各路由器的接口 IP 地址，在 PIM-SM 域内配置 OSPF 协议实现互联。
2. 启动组播功能，并在各接口上启动 PIM-SM 功能，在主机侧接口上使能 IGMP 功能。
3. 在 RouterC 和 RouterD 的 Loopback10 接口地址相同，配置 C-RP。在 Loopback1 接口上配置 C-BSR。
4. 在 RouterC 和 RouterD 的 Loopback0 接口上配置 MSDP 对等体。根据 RPF 规则，接受源 RP 发来的 SA 消息。

数据准备

为完成此配置例，需准备如下的数据：

- 组播组 G 地址：225.1.1.1/24。
- RouterC 的 router id 为 1.1.1.1。
- RouterD 的 router id 为 2.2.2.2。

操作步骤

步骤 1 配置各路由器的接口 IP 地址和单播路由协议

按照图 6-1，在 PIM-SM 域内，配置各路由器接口的 IP 地址和掩码，配置各路由器之间采用 OSPF 进行互连。具体配置过程略。

步骤 2 启动组播功能，并配置 PIM-SM 功能

在所有路由器上启动组播功能，并在各接口上启动 PIM-SM 功能，在主机侧接口使能 IGMP 功能。其他路由器上的配置过程与 RouterC 上的配置相似，配置过程略。

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

步骤 3 配置 Loopback1、Loopback10 接口，C-BSR、C-RP 的位置

在 RouterC 和 RouterD 上分别配置 Loopback1 接口地址和相同的 Loopback10 接口地址，在 Loopback1 上配置 C-BSR，在 Loopback10 上配置 C-RP。RouterD 上的配置过程与 RouterC 上的配置相似，配置过程略。

```
[RouterC] interface loopback 1
[RouterC-LoopBack1] ip address 3.3.3.3 255.255.255.255
[RouterC-LoopBack1] pim sm
[RouterC-LoopBack1] quit
[RouterC] interface loopback 10
[RouterC-LoopBack10] ip address 10.1.1.1 255.255.255.255
[RouterC-LoopBack10] pim sm
[RouterC-LoopBack10] quit
```

```
[RouterC] pim
[RouterC-pim] c-bsr loopback 1
[RouterC-pim] c-rp loopback 10
[RouterC-pim] quit
```

步骤 4 配置 Loopback0 接口和 MSDP 对等体

在 RouterC 上的 Loopback0 接口上配置 MSDP 对等体。

```
[RouterC] interface loopback 0
[RouterC-LoopBack0] ip address 1.1.1.1 255.255.255.255
[RouterC-LoopBack0] pim sm
[RouterC-LoopBack0] quit
[RouterC] msdp
[RouterC-msdp] originating-rp loopback0
[RouterC-msdp] peer 2.2.2.2 connect-interface loopback0
[RouterC-msdp] quit
```

在 RouterD 上的 Loopback0 接口上配置 MSDP 对等体。

```
[RouterD] interface loopback 0
[RouterD-LoopBack0] ip address 2.2.2.2 255.255.255.255
[RouterD-LoopBack0] pim sm
[RouterD-LoopBack0] quit
[RouterD] msdp
[RouterD-msdp] originating-rp loopback0
[RouterD-msdp] peer 1.1.1.1 connect-interface loopback0
[RouterD-msdp] quit
```

步骤 5 检验配置效果

通过使用 **display msdp brief** 命令可以查看路由器之间 MSDP 对等体建立情况。RouterC 和 RouterD 上 MSDP 对等体的显示信息如下：

```
[RouterC] display msdp brief
MSDP Peer Brief Information
  Configured   Up           Listen       Connect      Shutdown     Down
  1            1            0            0            0            0
  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  2.2.2.2            Up        00:10:17        ?      0          0
[RouterD] display msdp brief
MSDP Peer Brief Information
  Configured   Up           Listen       Connect      Shutdown     Down
  1            1            0            0            0            0
  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  1.1.1.1            Up        00:10:18        ?      0          0
```

通过使用 **display pim routing-table** 命令可以查看路由器上的 PIM 路由。PIM-SM 域内组播源 S1（10.110.5.100/24）向组播组 G（225.1.1.1）发送组播信息，用户 User1 加入组播组 G，接收发往组 G 的组播数据。通过比较 RouterC 和 RouterD 上 PIM 路由的显示信息，可知当前有效 RP 是 RouterC：S1 向 RouterC 注册，User1 向 RouterC 发起加入。

```
<RouterC> display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry
 (*, 225.1.1.1)
     RP: 10.1.1.1 (local)
     Protocol: pim-sm, Flag: WC
     UpTime: 00:28:49
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet3/0/0
             Protocol: static, UpTime: 00:28:49, Expires: -
 (10.110.5.1, 225.1.1.1)
```

```
    RP: 10.1.1.1 (local)
    Protocol: pim-sm, Flag: SPT 2MSDP ACT
    UpTime: 00:02:26
    Upstream interface: GigabitEthernet2/0/0
        Upstream neighbor: 10.110.1.2
        RPF prime neighbor: 10.110.1.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet3/0/0
            Protocol: pim-sm, UpTime: 00:02:26, Expires: -
<RouterD> display pim routing-table
```

无输出信息。

User1 退出组播组 G，S1 停止向组播组 G 发送组播数据。使用 **reset multicast routing-table all** 和 **reset multicast forwarding-table all** 清除 RouterC 上的组播路由表项和转发表项。

```
<RouterC> reset multicast routing-table all
<RouterC> reset multicast forwarding-table all
```

用户 User2 加入组播组 G，S2（10.110.6.100/24）开始向组播组 G 发送组播数据。通过比较 RouterC 和 RouterD 上 PIM 路由的显示信息，可知当前有效 RP 是 RouterD：S2 向 RouterD 注册，User2 向 RouterD 发起加入。

```
<RouterC> display pim routing-table
```

无输出信息。

```
<RouterD> display pim routing-table
VPN-Instance: public net
Total 1 (*, G) entry; 1 (S, G) entry
(*, 225.1.1.1)
    RP: 10.1.1.1 (local)
    Protocol: pim-sm, Flag: WC RPT
    UpTime: 00:07:23
    Upstream interface: NULL,
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet3/0/0,
            Protocol: pim-sm, UpTime: 00:07:23, Expires:-
 (10.110.6.100, 225.1.1.1)
    RP: 10.1.1.1 (local)
    Protocol: pim-sm, Flag: SPT 2MSDP ACT
    UpTime: 00:10:20
    Upstream interface: GigabitEthernet2/0/0
        Upstream neighbor: 10.110.2.2
        RPF prime neighbor: 10.110.2.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet3/0/0
            Protocol: pim-sm, UpTime: 00:10:22, Expires: -
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.110.5.1 255.255.255.0
```

```
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 10.110.1.2 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 10.110.5.0 0.0.0.255
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.110.6.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 10.110.2.2 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.6.0 0.0.0.255
  network 10.110.2.0 0.0.0.255
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 10.110.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 10.110.4.1 255.255.255.0
 igmp enable
 pim sm
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 pim sm
#
interface LoopBack10
 ip address 10.1.1.1 255.255.255.255
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 10.110.4.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
```

```
  network 3.3.3.3 0.0.0.0
  network 10.1.1.1 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
pim
 c-bsr LoopBack1
 c-rp LoopBack10
#
msdp
 originating-rp LoopBack0
 peer 2.2.2.2 connect-interface LoopBack0
#
return
```

- RouterD 的配置文件

```
#
 sysname RouterD
#
 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 10.110.2.1 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 10.110.3.1 255.255.255.0
 igmp enable
 pim sm
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 pim sm
#
interface LoopBack10
 ip address 10.1.1.1 255.255.255.255
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 10.110.3.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 10.1.1.1 0.0.0.0
  network 192.168.3.0 0.0.0.255
#
pim
 c-bsr LoopBack1
 c-rp LoopBack10
#
msdp
 originating-rp LoopBack0
 peer 1.1.1.1 connect-interface LoopBack0
#
return
```

- RouterE 的配置文件

```
#
 sysname RouterE
#
 multicast routing-enable
#
```

```
interface GigabitEthernet1/0/0
 ip address 10.110.3.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 10.110.1.2 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.3.0 0.0.0.255
  network 10.110.1.0 0.0.0.255
#
return
```

7 IPv4 组播路由管理

关于本章

系统可同时维护多个组播路由协议，通过控制平面与转发平面之间的信息交互，控制组播路由和转发。

7.1 IPv4 组播路由管理概述
组播路由与转发维护协议路由表、组播路由表和组播转发表。组播路由协议应用 RPF 机制创建组播路由表项。

7.2 AR2200-S 支持的 IPv4 组播路由管理特性
系统支持的 IPv4 组播路由管理特性包括：组播静态路由、GRE 隧道、组播路由策略、控制组播转发的范围、控制组播转发表的规模、组播路由测试、以及组播负载分担。

7.3 配置组播静态路由
组播静态路由实现的功能包括：改变 RPF 路由和衔接 RPF 路由。

7.4 配置组播路由策略
组播路由策略包括：配置组播路由最长匹配、配置组播负载分担及权值。

7.5 配置组播转发范围
网络中每个组播组对应的组播信息都要在一个确定的范围内传递。通过配置组播转发边界限制组播数据转发范围。

7.6 配置组播转发表限制参数
在进行网络规划时，可限定组播设备的转发表容量，包括：组播转发表最大表项数和组播转发表项最大下行节点数。从而缓解组播设备的处理压力，避免因表项过多引发的设备故障。

7.7 维护 IPv4 组播路由管理
IPv4 组播路由管理的维护包括：测试组播路由、检查 RPF 路径和组播路径、清除组播转发表项和路由表项。

7.8 配置举例
针对如何在组播网络中配置组播静态路由和组播负载分担，分别提供配置举例。

7.1 IPv4 组播路由管理概述

组播路由与转发维护协议路由表、组播路由表和组播转发表。组播路由协议应用 RPF 机制创建组播路由表项。

AR2200-S 的组播实现中，组播路由与转发分为三个方面：

- 每个组播路由协议有一个协议自身的路由表，如 PIM Routing-Table。
- 各个组播路由协议的组播路由信息经过综合形成一个总的组播路由表，即 Multicast Routing-Table。

  Multicast Routing-Table 是组播路由管理模块中的路由表，由一组（S，G）表项组成。（S，G）表示由源 S 向组播组 G 发送的组播数据的路由信息。如果组播路由管理支持多种组播协议，则路由表中将包括由多种协议生成的组播路由。路由表项直接下发到转发表中。
- 组播转发表直接控制着组播数据包的转发，即 Multicast Forwarding-Table。

  Multicast Forwarding-Table 是真正指导组播数据转发的组播转发表。组播转发表与组播路由表保持一致。

组播路由协议运用 RPF（Reverse Path Forwarding）机制创建组播路由表项，以确保组播数据能够沿正确的路径传输。

系统根据以下几种路由执行 RPF 检查：

- 单播路由

  单播路由表中汇集了到达各个目的地址的最短路径。
- MBGP 路由

  MBGP 路由表直接提供组播路由信息。
- MIGP 路由

  MIGP 路由表提供根据 TE Tunnel 的物理接口计算出的路由信息，以指导组播报文转发。
- 组播静态路由

  组播静态路由表中列举了用户通过静态配置指定的 RPF 路由信息。

7.2 AR2200-S 支持的 IPv4 组播路由管理特性

系统支持的 IPv4 组播路由管理特性包括：组播静态路由、GRE 隧道、组播路由策略、控制组播转发的范围、控制组播转发表的规模、组播路由测试、以及组播负载分担。

组播静态路由

组播静态路由是 RPF 检查的重要依据。通过配置组播静态路由，用户可以在当前路由器上为特定“报文源”指定 RPF 接口和 RPF 邻居。

组播静态路由不能用于数据转发，它可以用来改变 RPF 路由或衔接 RPF 路由。

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

GRE 隧道

网络中可能存在不支持组播的路由器。组播数据沿组播路由器逐跳转发，当下一跳路由器不支持组播时，组播路径将被阻断。这时，通过在两岸的组播路由器之间建立 GRE（Generic Routing Encapsulation）隧道，可以实现跨越单播网段传输组播数据。

组播路由策略

运行组播的路由器选择上游接口时，若存在多条开销相同的单播路由，用户可以设置路由器选取 RPF 路由的方式，有以下三种：

- 缺省情况下，选择下一跳地址最大的路由。
- 按照最长匹配原则，选取目的地址与“报文源”地址匹配最长的路由。
- 各路由之间负载分担。根据不同的策略进行组播流量的负载分担，可以优化存在多个组播数据流时的网络流量。

  组播负载分担策略共有 5 种：稳定优先、均衡优先、基于源地址、基于组地址、基于源/组地址。这 5 种负载分担策略是互斥的。在稳定优先和均衡优先负载分担方式中，还可以在接口上配置组播负载分担权值，实现组播不均衡负载分担。

控制组播转发的范围

网络中组播信息的转发不会是漫无边际的，每个组播组对应的组播信息都需要在一个确定的范围内传递。AR2200-S 允许用户通过以下方式定义组播转发范围：

- 在接口上配置组播转发边界，以形成一个封闭的组播转发区域。

控制组播转发表的规模

ISP 根据所提供的组播业务进行具体的网络规划时，可以进行如下的策略配置：

- 限制组播转发表中的表项数量

  路由器为每一个接收到的组播报文都维护有对应的转发表项。但是，过量的组播转发项将有可能会耗尽路由器内存。AR2200-S 允许用户自己定义路由器组播转发表项的最大数量。根据实际组网情况和业务性能对表项数量进行适当的限制，可以避免由此引发的路由器故障。
- 限制单个转发表项的下行节点数量

  路由器为每一个下行节点复制一份组播报文，发送出去。每一个下行节点形成组播分发树的一路分支。下行节点数决定了组播分发树可能达到的最大规模和组播服务范围。AR2200-S 允许用户自己定义单个转发表项的下行节点数量。根据实际组网情况和业务性能对下行节点数量进行适当的限制，可以缓解路由器的处理压力，并控制组播服务范围。

组播路由测试

当组播网络出现故障时，可以首先使用 **ping multicast** 与 **mtrace** 命令测试网络连接是否正常工作。

ping multicast 命令主要用于检查组播组是否可达，实现以下功能：

- Ping 保留组地址：用来检测直连网段上是否存在保留组成员，不仅限于组播网络，还可以 Ping 其他使用组播地址的设备。
- Ping 普通组播组地址，有以下两个作用：

- 构造组播流量，触发建立组播路由表项。用户通过查看组播路由信息来检查协议状态是否正常，判断网络是否具备承载组播业务的能力，或者测试转发性能。
- 检查网络中存在的组成员。发起 Ping 的路由器通过统计目的主机反馈的 ICMP-Echo-Reply 报文来确定网络中存在的哪些组成员、计算从 Ping 发起者到组成员的 TTL、响应时间等。还可以按照一定时间间隔多次发起 Ping，以计算网络时延和路由抖动。

mtrace 能够追踪以下 4 种路径，并输出逐跳信息。

- 从组播源到查询者的 RPF 路径
- 从组播源到查询者的组播路径
- 从组播源到目的主机的 RPF 路径
- 从组播源到目的主机的组播路径

7.3 配置组播静态路由

组播静态路由实现的功能包括：改变 RPF 路由和衔接 RPF 路由。

7.3.1 建立配置任务

在配置组播静态路由前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以快速、准确地完成配置任务。

应用环境

以具体应用环境区分，组播静态路由主要有两种功能：

- 改变 RPF 路由

  当网络中组播拓扑结构和单播拓扑结构相同时，组播数据的传输路径与单播相同。AR2200-S 允许用户配置组播静态路由，从而更改 RPF 路由，为组播数据创建一条与单播不同的传输路径。
- 衔接 RPF 路由

  在单播路由被阻断的网段，未配置组播静态路由时，由于没有 RPF 路由而无法进行报文转发。AR2200-S 允许用户配置组播静态路由，从而生成 RPF 路由、完成 RPF 检查，最终创建路由表项、指导报文转发。

前置任务

在配置组播静态路由之前，需完成以下任务：

- 配置某单播路由协议
- 配置基本组播功能

数据准备

在配置组播静态路由之前，需准备以下数据。

序号	数据
1	组播源地址、掩码/掩码长度

序号	数据
2	单播路由协议
3	过滤策略、优先级

7.3.2 配置组播静态路由功能

配置组播静态路由，可以在当前组播设备上指定 RPF 接口和 RPF 邻居。

背景信息

注意

配置组播静态路由时，若下一跳接口是点对点形式，则可在命令中配置出接口。若下一跳接口是非点对点形式，则必须使用下一跳地址形式。

在组播路由器上进行如下配置。

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 **ip rpf-route-static** *source-address* { *mask* | *mask-length* } [**isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**] [**route-policy** *route-policy-name*] { *rpf-nbr* | *interface-type interface-number* } [**preference** *preference*] [**order** *order-number*]，配置组播静态路由。

- *source-address* { *mask* | *mask-length* }是组播源地址及掩码。
- 指定 **isis** *process-id*、**ospf** *process-id*、**rip** *process-id*、、**static** 表示匹配的路由必须在指明的单播路由协议中出现。*process-id* 是进程号。
- **route-policy** *policy-name* 是静态组播路由的匹配规则。
- *rpf-nbr* 是下一跳地址，作为 RPF 邻居 IP 地址。
- *interface-type interface-number* 是出接口类型及编号，作为 RPF 接口。
- **preference** *preference* 是路由优先级，优先级数值越大，优先级越低。
- **order** *order-num* 是同网段路由中的配置先后次序。

----结束

7.3.3 检查配置结果

配置组播静态路由成功后，查看组播静态路由表以及 RPF 路由信息，确保组播网络正常运行。

操作步骤

- 使用 **display multicast routing-table static** [**config**] [*source-address* { *mask* | *mask-length* }]命令查看组播静态路由表信息。

- 使用 **display multicast rpf-info** *source-address* [*group-address*] [**rpt** | **spt**]命令查看指定组播源的 RPF 路由信息。

----结束

7.4 配置组播路由策略

组播路由策略包括：配置组播路由最长匹配、配置组播负载分担及权值。

7.4.1 建立配置任务

在配置组播路由策略前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以快速、准确地完成配置任务。

应用环境

当组播路由器选择上游接口时，可能存在多个开销相同的单播路由。用户可以根据具体的网络需要，从以下三种方法中任选其一，设置 RPF 路由的选择方法。

- 缺省情况下，选择下一跳地址最大的路由。
- 配置按照最长匹配原则，选取目的地址与“报文源”地址匹配最长的路由。
- 配置各路由之间的负载分担。根据不同的策略配置组播负载分担，可以优化存在多个组播数据流时的网络流量。

前置任务

在配置组播路由策略之前，需完成以下任务：

- 配置某单播路由协议
- 配置基本组播功能

数据准备

在配置组播路由策略之前，需准备以下数据。

序号	数据
1	组播负载分担的策略
2	接口的组播负载分担权值

7.4.2 配置组播路由最长匹配

按照最长匹配选择路由时，组播设备会优先选取目的地址与报文源地址匹配“掩码”最长的路由。若存在多条路由掩码匹配长度相同，则按照组播静态路由、域间单播路由、域内单播路由的顺序选择一条路由作为组播数据的转发路径。

背景信息

缺省情况下，按照路由表项的顺序来选择路由。

在组播路由器上进行如下配置。

操作步骤

- 1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **multicast longest-match**，配置按照最长匹配来选择路由。

----结束

7.4.3 配置组播负载分担

组播负载分担功能扩展了组播选路规则，不完全依赖 RPF 检查。根据不同的策略进行组播流量的负载分担，可以优化存在多个组播数据流时的网络流量。可选择使用均衡优先负载分担或稳定优先负载分担策略。

背景信息

组播负载分担功能扩展了组播选路规则，不完全依赖 RPF 检查。网络中存在多条等价的最优路由时，它们都可能用来转发组播数据，组播流量可以在多条等价路由间进行负载分担。

缺省情况下，没有配置组播负载分担。

在运行组播的路由器上进行如下配置。

操作步骤

- 1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **multicast load-splitting** { **balance-preferred** | **stable-preferred** | **source** | **group** | **source-group** }，配置组播负载分担。

     参数含义如下：

     - **balance-preferred**：表示均衡优先负载分担。该策略适用于组播业务频繁加入和退出，需要自动调整负载均衡的场景。

       增加或删除等价路由、删除组播路由表项、接口的组播负载分担权值变化时，路由器会对负载自动进行均衡调整。
     - **stable-preferred**：表示稳定优先负载分担。该策略适用于组播业务稳定的场景。

       增加或删除等价路由时，路由器会对负载自动进行均衡调整。删除组播路由表项、接口的组播负载分担权值变化时，路由器不主动对负载进行均衡调整。
     - **group**：表示基于组地址进行负载分担。该策略适用于一源多组的场景。
     - **source**：表示基于源地址进行负载分担。该策略适用于一组多源的场景。
     - **source-group**：表示同时基于源地址和组地址进行负载分担。该策略适用于多个源和多个组的场景。

说明

建议根据网络实际情况，固定选用一种组播负载分担策略。推荐使用 **balance-preferred** 或 **stable-preferred** 参数。

当一个实例下存在使能了 PIM-DM 的接口时，不能配置 **balance-preferred** 或 **stable-preferred** 参数。

配置组播负载分担均衡调整定时器的时间间隔和组播负载分担权值适用于稳定优先负载分担和均衡优先负载分担场景。

3. （可选）执行命令 **multicast load-splitting-timer** *interval*，配置组播负载分担均衡调整定时器的时间间隔。
4. （可选）执行命令 **interface** *interface-type interface-number*，进入接口视图。

----结束

7.4.4 检查配置结果

配置组播路由策略成功后，查看组播路由表以及 RPF 路由信息，确保组播网络正常运行。

操作步骤

- 使用 **display multicast routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** }] * [**outgoing-interface-number** [*number*]]命令查看组播路由表信息：
- 使用 **display multicast rpf-info** *source-address* [*group-address*] [**rpt** | **spt**]命令查看指定组播源的 RPF 路由信息。

----结束

7.5 配置组播转发范围

网络中每个组播组对应的组播信息都要在一个确定的范围内传递。通过配置组播转发边界限制组播数据转发范围。

7.5.1 建立配置任务

在配置组播转发范围前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以快速、准确地完成配置任务。

应用环境

网络中每个组播组对应的组播信息都需要在一个确定的范围内传递。AR2200-S 允许用户通过以下方式定义组播转发范围：

- 在接口上配置组播转发边界，以形成一个封闭的组播转发区域。当路由器接口配置了针对某组播组的转发边界以后，将不能再发出或接收该组播组的报文。

前置任务

在配置组播转发范围之前，需完成以下任务：

- 配置某单播路由协议
- 配置基本组播功能

数据准备

在配置组播转发范围之前，需准备以下数据。

序号	数据
1	组播转发边界的组地址、掩码/掩码长度

7.5.2 配置组播转发边界

当组播设备接口配置了针对某组播组的转发边界后，可以划定组播报文的转发范围。

背景信息

缺省情况下，接口未设置组播转发边界。

在组播路由器上进行如下配置。

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 **multicast boundary** *group-address* { *mask* | *mask-length* }，配置组播转发边界。

----结束

7.5.3 检查配置结果

配置组播转发范围成功后，查看组播路由表信息、接口的组播边界信息、以及接口转发 TTL 阈值，确保组播网络正常运行。

操作步骤

- 使用以下命令查看组播路由表信息：
  - **display multicast routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** }] * [**outgoing-interface-number** [*number*]]
- 使用 **display multicast boundary** [*group-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*]命令查看接口的组播边界信息。

----结束

7.6 配置组播转发表限制参数

在进行网络规划时，可限定组播设备的转发表容量，包括：组播转发表最大表项数和组播转发表项最大下行节点数。从而缓解组播设备的处理压力，避免因表项过多引发的设备故障。

7.6.1 建立配置任务

在配置组播转发表限制参数前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以快速、准确地完成配置任务。

应用环境

ISP 根据所提供的组播业务进行具体的网络规划时，通常需要进行如下的策略配置：

- 限制组播转发表中的表项数量

  路由器为每一个接收到的组播报文都维护有对应的转发表项。但是，过量的组播转发项将有可能会耗尽路由器内存。AR2200-S 允许用户自己定义路由器组播转发表项的最大数量。根据实际组网情况和业务性能对表项数量进行适当的限制，可以避免由此引发的路由器故障。
- 限制单个转发表项的下行节点数量

  路由器为每一个下行节点复制一份组播报文，发送出去。每一个下行节点形成组播分发树的一路分支。下行节点数决定了组播分发树可能达到的最大规模和组播服务范围。AR2200-S 允许用户自己定义单个转发表项的下行节点数量。根据实际组网情况和业务性能对下行节点数量进行适当的限制，可以缓解路由器的处理压力，并控制组播服务范围。

前置任务

在配置组播转发表限制参数之前，需完成以下任务：

- 配置某单播路由协议
- 配置基本组播功能

数据准备

在配置组播转发表限制参数之前，需准备以下数据。

序号	数据
1	组播转发表中最大表项数目
2	组播转发表中每条路由项的最大下行节点数目

7.6.2 配置组播转发表最大表项数

过量的组播转发项可能会耗尽设备内存。系统允许用户配置组播设备转发表项的最大数量。根据实际组网情况和业务性能对表项数量进行适当限制，从而避免由此引发的设备故障。

背景信息

缺省情况下，采用路由器系统允许的最大值。

在组播路由器上进行如下配置。

操作步骤

- 公网实例
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **multicast forwarding-table route-limit** *limit*，配置组播转发表最大表项数。

----结束

7.6.3 配置组播转发表项最大下行节点数

组播设备为每一个下行节点复制一份组播报文。系统允许用户定义单个转发表项的最大下行节点数量。根据实际组网情况和业务性能对下行节点数量进行适当限制，从而缓解组播设备的处理压力。

背景信息

注意

该配置在执行命令 **reset multicast forwarding-table** 后才生效，执行 **reset multicast forwarding-table** 命令会导致组播业务中断，请谨慎使用。

在组播路由器上进行如下配置。

操作步骤

- 公网实例
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **multicast forwarding-table downstream-limit** *limit*，配置组播转发表中单条路由项的最大下行节点数目。配置值小于系统缺省值时有效。

----结束

7.6.4 检查配置结果

配置组播转发表限制参数成功后，查看组播转发表信息，确保组播网络正常运行。

操作步骤

步骤 1 使用 **display multicast forwarding-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** |

exclude | **match** } { *interface-type interface-number* | **register** | **none** } | **statistics**] *命令查看组播转发表信息。

----结束

7.7 维护 IPv4 组播路由管理

IPv4 组播路由管理的维护包括：测试组播路由、检查 RPF 路径和组播路径、清除组播转发表项和路由表项。

7.7.1 测试组播路由

当组播数据传输出现故障时，选择执行 ping 命令查看 RPF 路径和组播路径。

背景信息

当组播数据传输出现故障时，可以通过执行以下命令查看 RPF 路径和组播路径。

操作步骤

- 使用 **ping multicast** [**-i** *interface-type interface-number* | **-c** *count* | **-h** *ttl-value* | **-m** *time* | **-p** *pattern* | **-q** | **-s** *packet（s）ize* | **-t** *timeout* | **-tos** *tos-value* | **-v**] * *host* 命令 Ping 保留组地址。
- 使用 **ping multicast** [**-c** *count* | **-h** *ttl-value* | **-m** *time* | **-p** *pattern* | **-q** | **-s** *packet（s）ize* | **-t** *timeout* | **-tos** *tos-value* | **-v**] * *host* 命令 Ping 普通组地址。

----结束

7.7.2 检查 RPF 路径和组播路径

当组播数据传输出现故障时，选择执行 mtrace 命令查看 RPF 路径和组播路径。

背景信息

说明

查看从组播源到目的主机的 RPF 路径或者组播路径时，需要在连接用户主机的路由器上执行命令 **mtrace query-policy** [*acl-number*]，配置查询者过滤策略。ACL 限定了可信任的查询者的地址范围，最后一跳路由器依据该 ACL 拒绝非法查询者发出的 IGMP-Tracert-Query 消息。使用该命令有以下注意事项：

- 该命令只在最后一跳路由器上生效，且查询者不是最后一跳路由器。
- 该命令只对使用单播 IP 报文封装的 IGMP-Tracert-Query 消息进行过滤。
- 该命令不适用于从查询者本地发起的追踪。

当组播数据传输出现故障时，可以通过执行以下命令查看 RPF 路径和组播路径。

操作步骤

- 使用 **mtrace** [**-ur** *resp-dest* | **-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout*] * **source** *source-address* 命令查看从组播源到查询者的 RPF 路径。

- 使用 **mtrace -g** *group* [{ **-mr** | **-ur** *resp-dest* } | **-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout*] * **source** *source-address* 命令查看从组播源到查询者的组播路径。
- 使用 **mtrace** { **-gw** *last-hop-router* | **-d** } **-r** *receiver* [**-ur** *resp-dest* | **-a** *source-ip-address* | **-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout*] * **source** *source-address* 命令看从组播源到目的主机的 RPF 路径。
- 使用 **mtrace** { **-gw** *last-hop-router* | **-b** | **-d** } **-r** *receiver* **-g** *group* [{ **-mr** | **-ur** *resp-dest* } | **-a** *source-ip-address* | **-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout*] * **source** *source-address* 命令查看从组播源到目的主机的组播路径。

----结束

7.7.3 清除组播转发表项和路由表项

在确认需要清除组播转发表项和路由表项后，在用户视图下选择执行 reset 命令,清除组播转发表项和路由表项。执行 reset 命令将删除组播转发表或路由表中的信息，可能导致组播数据无法正常传输,请慎用。

背景信息

注意

执行 **reset** 命令将删除组播转发表或路由表中的信息，可能导致组播数据无法正常传输。清除公网实例的组播路由表中的路由项后，公网实例的相应组播转发项也将被删除。

在确认需要清除组播转发表和路由表的运行信息后，请在用户视图下执行下面的 **reset** 命令。

操作步骤

- 请在用户视图下执行以下命令清除组播转发表中的转发项：
  - **reset multicast forwarding-table all**
  - **reset multicast forwarding-table** { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } *
- 请在用户视图下执行以下命令清除组播路由表的路由项：
  - **reset multicast routing-table all**
  - **reset multicast routing-table** { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } *

----结束

7.8 配置举例

针对如何在组播网络中配置组播静态路由和组播负载分担，分别提供配置举例。

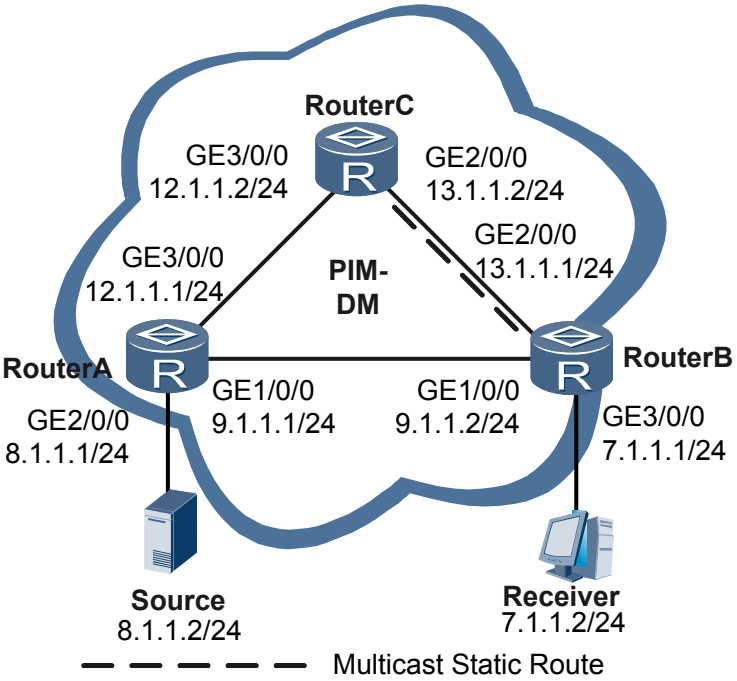
7.8.1 配置组播静态路由改变 RPF 路由示例

在组播网络中配置组播静态路由改变 RPF 路由，使组播源到接收者的组播路径与单播路径不同，为组播创建一条与单播不同的传输路径。

组网需求

如图 7-1 所示，网络中运行 PIM-DM，所有路由器都支持组播，且 Receiver 能够正常接收组播源 Source 的信息。RouterA、RouterB 和 RouterC 之间运行 OSPF 协议。要求：使用组播静态路由，使 Source 到 Receiver 的组播路径与单播路径不同。

图 7-1 配置组播静态路由改变 RPF 路由组网图



配置思路

采用如下的思路配置组播静态路由：

1. 配置各路由器的接口 IP 地址和 OSPF 单播路由协议。
2. 使能组播功能，在各接口上使能 PIM-DM，在与主机相连的接口上使能 IGMP。
3. 在 RouterB 上配置 RPF 组播静态路由，指定到源的 RPF 邻居为 RouterC。

数据准备

为完成此配置举例，需准备如下的数据：

- Source 的 IP 地址。
- 路由器各接口的 IP 地址。

操作步骤

步骤 1 配置各路由器的接口 IP 地址和单播路由协议

按照图 7-1 配置各路由器接口的 IP 地址和掩码。RouterA、RouterB 和 RouterC 之间运行 OSPF，能够借助单播路由协议实现动态路由更新。配置过程略。

步骤 2 使能组播功能，并在各接口上使能 PIM-DM 功能

在所有路由器上启动组播功能，并在各接口上使能 PIM-DM 功能，主机侧接口上使能 IGMP 功能。其他路由器上 PIM-DM 功能的配置过程与 RouterB 上的配置相似，配置过程略。

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

在 RouterB 上执行 **display multicast rpf-info** 命令，查看 Source 的 RPF 路由信息。发现当前 RPF 路由来源于 unicast，RPF 邻居是 RouterA。信息显示如下：

```
<RouterB> display multicast rpf-info 8.1.1.2
VPN-Instance: public net
RPF information about source: 8.1.1.2
     RPF interface: GigabitEthernet1/0/0, RPF neighbor: 9.1.1.1
     Referenced route/mask: 8.1.1.0/24
     Referenced route type: unicast
     Route selection rule: preference-preferred
     Load splitting rule: disabled
```

步骤 3 配置组播静态路由

在 RouterB 上配置 RPF 组播静态路由，到 Source 的 RPF 邻居为 RouterC。

```
[RouterB] ip rpf-route-static 8.1.1.0 255.255.255.0 13.1.1.2
```

步骤 4 检验配置效果

在 RouterB 上执行 **display multicast rpf-info** 命令，查看 Source 的 RPF 信息。RPF 信息显示如下。与配置组播静态路由前比较，RPF 路由与 RPF 邻居已经依据静态路由更新。

```
<RouterB> display multicast rpf-info 8.1.1.2
VPN-Instance: public net
RPF information about source: 8.1.1.2
     RPF interface: GigabitEthernet2/0/0, RPF neighbor: 13.1.1.2
     Referenced route/mask: 8.1.1.0/24
     Referenced route type: mstatic
     Route selection rule: preference-preferred
     Load splitting rule: disabled
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
```

```
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 9.1.1.1 255.255.255.0
 pim dm
#
interface GigabitEthernet2/0/0
 ip address 8.1.1.1 255.255.255.0
 pim dm
#
interface GigabitEthernet3/0/0
 ip address 12.1.1.1 255.255.255.0
 pim dm
#
ospf 1
 area 0.0.0.0
  network 12.1.1.0 0.0.0.255
  network 9.1.1.0 0.0.0.255
  network 8.1.1.0 0.0.0.255
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 9.1.1.2 255.255.255.0
 pim dm
#
interface GigabitEthernet2/0/0
 ip address 13.1.1.1 255.255.255.0
 pim dm
#
interface GigabitEthernet3/0/0
 ip address 7.1.1.1 255.255.255.0
 pim dm
 igmp enable
#
ospf 1
 area 0.0.0.0
  network 7.1.1.0 0.0.0.255
  network 9.1.1.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
#
ip rpf-route-static 8.1.1.0 255.255.255.0 13.1.1.2
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
 multicast routing-enable
#
interface GigabitEthernet2/0/0
 ip address 13.1.1.2 255.255.255.0
 pim dm
#
interface GigabitEthernet3/0/0
 ip address 12.1.1.2 255.255.255.0
 pim dm
#
ospf 1
 area 0.0.0.0
  network 13.1.1.0 0.0.0.255
  network 12.1.1.0 0.0.0.255
```

```
#
return
```

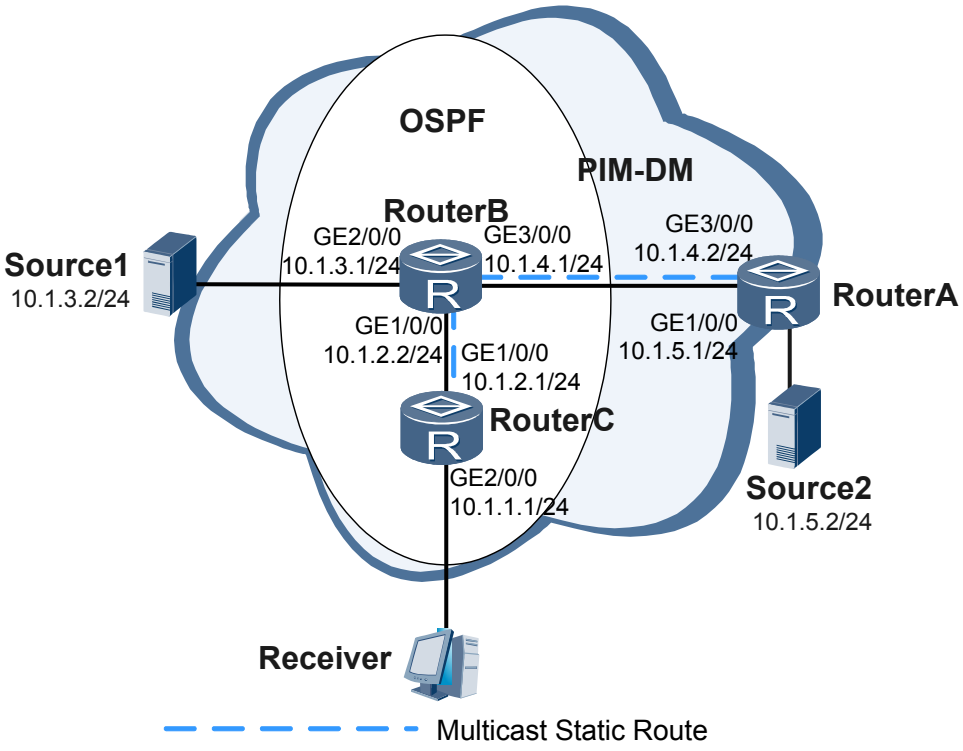
7.8.2 配置组播静态路由衔接 RPF 路由示例

在组播网络中配置组播静态路由，使接收者能够接收到与本区域单播路由隔离的其他区域组播源的组播数据。

组网需求

如图 7-2 所示，网络中运行 PIM-DM，所有路由器都支持组播，且 Receiver 能够能正常接收组播源 Source1 的信息。RouterB 和 RouterC 之间运行 OSPF 协议，并与 RouterA 单播路由隔离。要求：使用组播静态路由，使 Receiver 能够接收 OSPF 域外组播源 Source2 的信息。

图 7-2 配置组播静态路由衔接 RPF 路由组网图



配置思路

采用如下的思路配置组播静态路由：

1. 配置各路由器的接口 IP 地址和 OSPF 单播路由协议。
2. 使能组播功能，并在各接口上使能 PIM-DM 功能，在主机侧接口上使能 IGMP 功能。
3. 在 RouterB 和 RouterC 上配置 RPF 组播静态路由。

数据准备

为完成此配置举例，需准备如下的数据：

- Source2 的 IP 地址。
- RouterB 上到 Source2 的 RPF 接口为 GE3/0/0，RPF 邻居为 RouterA。
- RouterC 上到 Source2 的 RPF 接口为 GE1/0/0，RPF 邻居为 RouterB。

操作步骤

步骤 1 配置各路由器的接口 IP 地址和单播路由协议

按照图 7-2 配置各路由器接口的 IP 地址和掩码。RouterB 和 RouterC 属于同一 OSPF 区域，并且之间能够借助单播路由协议实现动态路由更新。配置过程略。

步骤 2 使能组播功能，并在各接口上使能 PIM-DM 功能

在所有路由器上启动组播功能，并在各接口上使能 PIM-DM，在与主机相连的接口上使能 IGMP。

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

Source1（10.1.3.2/24）和 Source2（10.1.5.2/24）都向组播组 G（225.1.1.1）发送组播数据。Receiver 加入组 G，能够收到 Source1 发出的组播数据，收不到 Source2 发出的组播数据。

分别在 RouterB 和 RouterC 上执行 **display multicast rpf-info 10.1.5.2** 命令，没有显示信息。说明路由器上没有到 Source2 的 RPF 路由。

步骤 3 配置组播静态路由

在 RouterB 上配置 RPF 组播静态路由，到 Source2 的 RPF 邻居为 RouterA。

```
[RouterB] ip rpf-route-static 10.1.5.0 255.255.255.0 10.1.4.2
```

在 RouterC 上配置 RPF 组播静态路由，到 Source2 的 RPF 邻居为 RouterB。

```
[RouterC] ip rpf-route-static 10.1.5.0 255.255.255.0 10.1.2.2
```

步骤 4 检验配置效果

分别在 RouterB 和 RouterC 上执行 **display multicast rpf-info 10.1.5.2** 命令，查看 Source2 的 RPF 信息。RPF 信息显示如下。

```
<RouterB> display multicast rpf-info 10.1.5.2
VPN-Instance: public net
RPF information about source: 10.1.5.2
     RPF interface: GigabitEthernet3/0/0, RPF neighbor: 10.1.4.2
     Referenced route/mask: 10.1.5.0/24
     Referenced route type: mstatic
     Route selecting rule: preference-preferred
     Load splitting rule: disabled
<RouterC> display multicast rpf-info 10.1.5.2
VPN-Instance: public net
RPF information about source: 10.1.5.2
     RPF interface: GigabitEthernet1/0/0, RPF neighbor: 10.1.2.2
     Referenced route/mask: 10.1.5.0/24
     Referenced route type: mstatic
     Route selection rule: preference-preferred
     Load splitting rule: disabled
```

在 RouterC 上执行 **display pim routing-table** 命令，查看路由表信息。RouterC 上存在 Source2 的组播表项。Receiver 正常接收来自 Source2 的组播数据。

```
<RouterC> display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 2 (S, G) entries
 (*, 225.1.1.1)
     Protocol: pim-dm, Flag: WC
     UpTime: 03:54:19
     Upstream interface: NULL
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet2/0/0
             Protocol: pim-dm, UpTime: 01:38:19, Expires: never
(10.1.3.2, 225.1.1.1)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:00:44
     Upstream interface: GigabitEthernet1/0/0
         Upstream neighbor: 10.1.2.2
         RPF prime neighbor: 10.1.2.2
     Downstream interface(s) information:
     Total number of downstreams: 1
          1: GigabitEthernet2/0/0
              Protocol: pim-dm, UpTime: 00:00:44, Expires: never
(10.1.5.2, 225.1.1.1)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:00:44
     Upstream interface: GigabitEthernet1/0/0
         Upstream neighbor: 10.1.2.2
         RPF prime neighbor: 10.1.2.2
     Downstream interface(s) information:
     Total number of downstreams: 1
          1: GigabitEthernet2/0/0
              Protocol: pim-dm, UpTime: 00:00:44, Expires: never
```

----结束

配置文件

- RouterA 的配置文件

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

```
 ip address 10.1.5.1 255.255.255.0
 pim dm
#
interface GigabitEthernet3/0/0
 ip address 10.1.4.2 255.255.255.0
 pim dm
#
ospf 1
 area 0.0.0.0
  network 10.1.5.0 0.0.0.255
  network 10.1.4.0 0.0.0.255
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.1.2.2 255.255.255.0
 pim dm
#
interface GigabitEthernet2/0/0
 ip address 10.1.3.1 255.255.255.0
 pim dm
#
interface GigabitEthernet3/0/0
 ip address 10.1.4.1 255.255.255.0
 pim dm
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 10.1.3.0 0.0.0.255
#
ip rpf-route-static 10.1.5.0 24 10.1.4.2
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.1.2.1 255.255.255.0
 pim dm
#
interface GigabitEthernet2/0/0
 ip address 10.1.1.1 255.255.255.0
 igmp enable
 pim dm
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
#
ip rpf-route-static 10.1.5.0 24 10.1.2.2
#
return
```

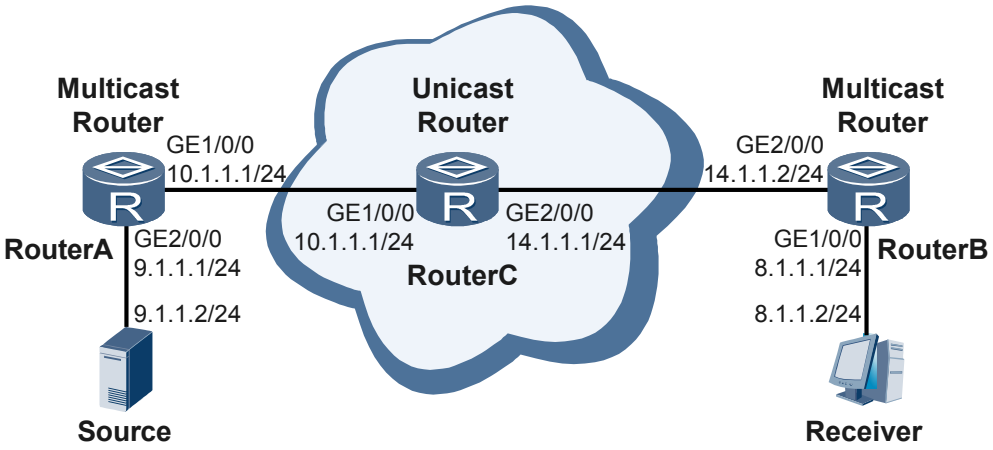
7.8.3 配置组播静态路由隧道实现组播示例

网络中存在不支持组播的区域，配置组播静态路由建立组播隧道可以实现组播数据跨越非组播区域的转发。

组网需求

如图 7-3 所示，网络中运行 PIM-DM，路由器 A 和 B 支持组播，路由器 C 不支持组播，Receiver 不能正常接收组播源 Source 的信息。RouterA、RouterB 和 RouterC 之间运行 OSPF 协议。要求：使用组播静态路由，使 Receiver 能够接收到组播源 Source 的信息。

图 7-3 配置组播静态路由隧道实现组播组网图



配置思路

采用如下的思路配置组播静态路由隧道实现组播：

- 配置各路由器的接口 IP 地址。
- 在 RouterA 和 RouterB 之间建立 GRE 隧道。
- 配置 OSPF 单播路由协议，使 RouterA、RouterB 和 RouterC 单播互通。
- 在 RouterA 和 RouterB 上使能组播功能，并在各接口上使能 PIM-DM 功能，在主机侧接口上使能 IGMP 功能。
- 在 RouterB 上配置 RPF 组播静态路由，指定 RPF 邻居为 RouterA。

数据准备

为完成此配置举例，需准备如下的数据：

- Source 的 IP 地址
- 路由器各接口的 IP 地址

操作步骤

步骤 1 配置各路由器的接口 IP 地址

按照图 7-3 配置各路由器接口的 IP 地址和掩码，配置过程略。

步骤 2 在 RouterA 和 RouterB 之间建立 GRE 隧道

RouterA 的配置如下：

```
[RouterA] interface tunnel 0/0/1
[RouterA-Tunnel0/0/1] ip address 20.1.1.1 24
[RouterA-Tunnel0/0/1] tunnel-protocol gre
[RouterA-Tunnel0/0/1] source 10.1.1.1
[RouterA-Tunnel0/0/1] destination 14.1.1.2
[RouterA-Tunnel0/0/1] quit
```

RouterB 的配置如下：

```
[RouterB] interface tunnel 0/0/1
[RouterB-Tunnel0/0/1] ip address 20.1.1.2 24
[RouterB-Tunnel0/0/1] tunnel-protocol gre
[RouterB-Tunnel0/0/1] source 14.1.1.2
[RouterB-Tunnel0/0/1] destination 10.1.1.1
[RouterB-Tunnel0/0/1] quit
```

步骤 3 配置 OSPF，使 RouterA、RouterB、RouterC 能够单播互通

在 RouterA 的配置 OSPF。

```
[RouterA] ospf 1
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 20.1.1.1 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

在 RouterB 的配置 OSPF。

```
[RouterB] ospf 1
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 14.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 8.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 20.1.1.2 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

在 RouterC 的配置 OSPF。

```
[RouterC] ospf 1
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 14.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

步骤 4 在 RouterA 和 RouterB 上使能组播功能，并在各接口上使能 PIM-DM 功能

在 RouterA 和 RouterB 上启动组播功能，并在各接口上使能 PIM-DM，在与主机相连的接口上使能 IGMP。

RouterA 的配置如下：

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

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] pim dm
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface tunnel 0/0/1
[RouterA-Tunnel0/0/1] pim dm
[RouterA-Tunnel0/0/1] quit
```

RouterB 的配置如下：

```
[RouterB] multicast routing-enable
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] pim dm
[RouterB-GigabitEthernet2/0/0] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] pim dm
[RouterB-GigabitEthernet1/0/0] igmp enable
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface tunnel 0/0/1
[RouterB-Tunnel0/0/1] pim dm
[RouterB-Tunnel0/0/1] quit
```

步骤 5 配置组播静态路由

在 RouterB 上配置 RPF 组播静态路由，使 RPF 邻居变为 RouterA。

```
[RouterB] ip rpf-route-static 9.1.1.0 255.255.255.0 20.1.1.1
```

步骤 6 检验配置效果

Source（9.1.1.2/24）向组播组 G（225.1.1.1）发送组播数据。Receiver 加入组 G，能够收到 Source1 发出的组播数据. 在 RouterB 上执行 **display pim routing-table** 命令，查看路由表信息。

```
<RouterB> display pim routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry
 (9.1.1.2, 225.1.1.1)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:13:29
     Upstream interface: Tunnel0/0/1
         Upstream neighbor: 20.1.1.1
         RPF prime neighbor: 20.1.1.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/0
               Protocol: pim-dm, UpTime:  -, Expires:  -
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
 pim dm
#
interface GigabitEthernet2/0/0
 ip address 9.1.1.1 255.255.255.0
 pim dm
#
interface Tunnel0/0/1
 ip address 20.1.1.1 255.255.255.0
```

```
 tunnel-protocol gre
 source 10.1.1.1
 destination 14.1.1.2
 pim dm
#
ospf 1
 area 0.0.0.0
  network 9.1.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
  network 20.1.1.1 0.0.0.255
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 8.1.1.1 255.255.255.0
 pim dm
 igmp enable
#
interface GigabitEthernet2/0/0
 ip address 14.1.1.2 255.255.255.0
 pim dm
#
interface Tunnel0/0/1
 ip address 20.1.1.2 255.255.255.0
 tunnel-protocol gre
 source 14.1.1.2
 destination 10.1.1.1
 pim dm
#
ospf 1
 area 0.0.0.0
  network 8.1.1.0 0.0.0.255
  network 14.1.1.0 0.0.0.255
  network 20.1.1.1 0.0.0.255
#
 ip rpf-route-static 9.1.1.0 255.255.255.0 20.1.1.1
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 14.1.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 14.1.1.0 0.0.0.255
#
return
```

7.8.4 配置组播负载分担示例

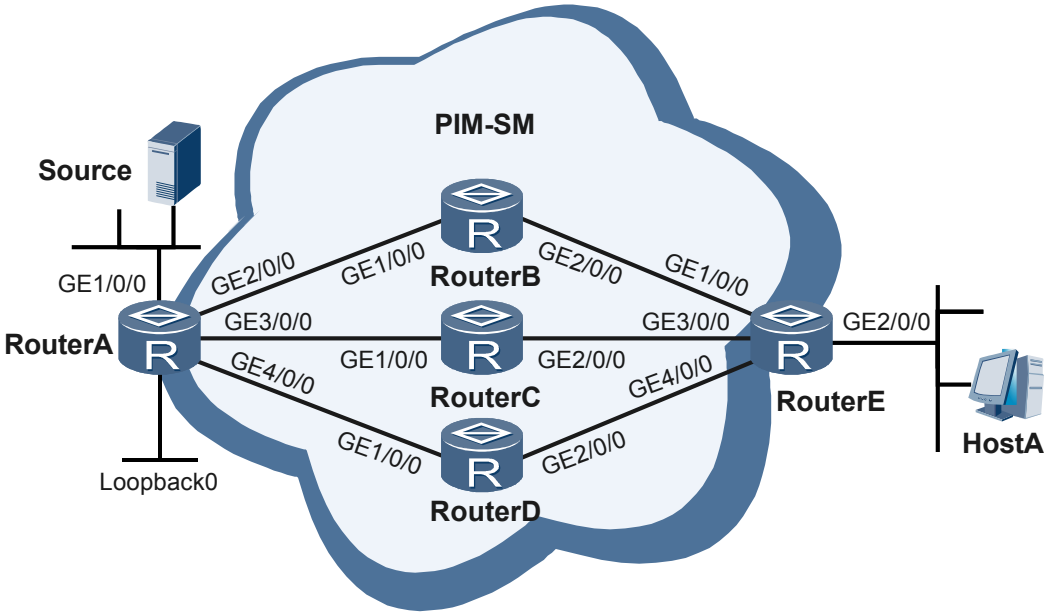
在组播网络中配置稳定优先组播负载分担策略，实现组播流量在多条等价路由间进行负载分担。

组网需求

如图 7-4 所示，与 HostA 相连的设备 RouterE 到组播源 Source 之间存在 3 条等价路由，在 RouterE 上配置稳定优先负载分担策略，可以将表项平均分布在各条等价路由上，从而实现各等价路由上的负载均衡。

若 RouterE 所在的三条等价路由的转发能力或流量拥塞程度不同，那么继续对组播表项进行均衡负载不能满足网络要求。在 RouterE 上配置不均衡负载分担，为其上游接口配置不同的负载分担权值，改变分布在各等价路由上的表项数量，实现对不同等价路由上表项数量的灵活控制。

图 7-4 配置组播负载分担组网图



设备	接口	IP 地址	设备	接口	IP 地址
RouterA	GE1/0/0	10.110.1.2/24	RouterC	GE1/0/0	192.168.2.2/24
	GE2/0/0	192.168.1.1/24		GE2/0/0	192.168.5.1/24
	GE3/0/0	192.168.2.1/24	RouterD	GE1/0/0	192.168.3.2/24
	GE4/0/0	192.168.3.1/24		GE2/0/0	192.168.6.1/24
	LoopBack0	1.1.1.1/32	RouterE	GE1/0/0	192.168.4.2/24
RouterB	GE1/0/0	192.168.1.2/24		GE3/0/0	192.168.5.2/24
	GE2/0/0	192.168.4.1/24		GE4/0/0	192.168.6.2/24
				GE2/0/0	10.110.2.2/24

配置思路

采用如下的思路配置组播负载分担：

- 配置各路由器的接口 IP 地址。

- 配置 IS-IS 协议，使所有路由器单播互通，且所有路由开销相同。
- 在所有路由器上使能组播功能，并在各接口上使能 PIM-SM，将 RouterA 的环回接口配置为 RP。
- 为了保证组播业务的稳定可靠，在 RouterE 上配置稳定优先组播负载分担。
- HostA 需要长期接收某些组播组的数据。配置 RouterE 的主机侧接口以静态方式批量加入组播组。
- HostA 需要接收新的组播组数据。根据网络需要为 RouterE 的各上游接口配置不同的组播负载分担权值，实现不均衡负载分担。

数据准备

为完成此配置例，需准备如下的数据：

- Source 的 IP 地址
- 各路由器的接口 IP 地址
- RouterE 的主机侧接口以静态方式批量加入的组播组地址
- RouterE 的各上游接口的组播负载分担权值

操作步骤

步骤 1 按照图 7-4 配置各路由器的接口 IP 地址（略）

步骤 2 配置 IS-IS 协议，使所有路由器单播互通，且所有路由开销相同（略）

步骤 3 在所有路由器上使能组播功能，并在各接口上使能 PIM-SM

配置 RouterA。RouterB、RouterC、RouterD 和 RouterE 上的配置与 RouterA 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
[RouterA] interface gigabitethernet 4/0/0
[RouterA-GigabitEthernet4/0/0] pim sm
[RouterA-GigabitEthernet4/0/0] quit
[RouterA] interface loopback 0
[RouterA-LoopBack0] pim sm
[RouterA-LoopBack0] quit
```

步骤 4 在 RouterA 上配置 RP

配置 RouterA 的 Loopback0 接口为 RP 地址。

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

步骤 5 在 RouterE 上配置稳定优先组播负载分担

```
[RouterE] multicast load-splitting stable-preferred
```

步骤 6 配置 RouterE 的主机侧接口以静态方式批量加入组播组

配置接口 GE2/0/0 以静态方式加入组播组 225.1.1.1 ～ 225.1.1.3。

```
[RouterE] interface gigabitethernet 2/0/0
[RouterE-GigabitEthernet2/0/0] igmp static-group 225.1.1.1 inc-step-mask 32 number 3
[RouterE-GigabitEthernet2/0/0] quit
```

步骤 7 验证稳定优先组播负载分担的配置结果

Source（10.110.1.1/24）向组播组 225.1.1.1 ～ 225.1.1.3 发送组播数据。HostA 能够收到 Source 发出的组播数据。在 RouterE 上查看 PIM 路由表的概要信息。

```
<Huawei> display pim routing-table brief
  VPN-Instance: public net
 Total 3 (*, G) entry; 3 (S, G) entries

  00001.(*, 225.1.1.1)
       Upstream interface:GE4/0/0
       Number of downstream:1
       Number of receive vrf:0
  00002.(10.110.1.1, 225.1.1.1)
       Upstream interface:GE4/0/0
       Number of downstream:1
       Number of receive vrf:0
  00003.(*, 225.1.1.2)
       Upstream interface:GE3/0/0
       Number of downstream:1
       Number of receive vrf:0
  00004.(10.110.1.1, 225.1.1.2)
       Upstream interface:GE3/0/0
       Number of downstream:1
       Number of receive vrf:0
  00005.(*, 225.1.1.3)
       Upstream interface:GE1/0/0
       Number of downstream:1
       Number of receive vrf:0
  00006.(10.110.1.1, 225.1.1.3)
       Upstream interface:GE1/0/0
       Number of downstream:1
       Number of receive vrf:0
```

(*,G)和(S,G)表项平均分布在三条等价路由上，上游接口分别为 GigabitEthernet4/0/0、GigabitEthernet3/0/0 和 GigabitEthernet1/0/0。

说明

负载分担算法对(*,G)和(S,G)表项分别处理，且处理规则相同。

步骤 8 为 RouterE 的各上游接口配置不同的组播负载分担权值，实现组播不均衡负载分担

配置接口 GigabitEthernet1/0/0 的组播负载分担权值为 2。

```
[RouterE] interface gigabitethernet 1/0/0
[RouterE-GigabitEthernet1/0/0] multicast load-splitting weight 2
[RouterE-GigabitEthernet1/0/0] quit
```

配置接口 GigabitEthernet4/0/0 的组播负载分担权值为 0。

```
[RouterE] interface gigabitethernet 4/0/0
[RouterE-GigabitEthernet4/0/0] multicast load-splitting weight 0
[RouterE-GigabitEthernet4/0/0] quit
```

步骤 9 配置 RouterE 的主机侧接口以静态方式批量加入新的组播组

配置接口 GE2/0/0 以静态方式加入组播组 225.1.1.4 ～ 225.1.1.9。

```
[RouterE] interface gigabitethernet 2/0/0
[RouterE-GigabitEthernet2/0/0] igmp static-group 225.1.1.4 inc-step-mask 32 number 6
[RouterE-GigabitEthernet2/0/0] quit
```

步骤 10 验证组播不均衡负载分担的配置结果

Source（10.110.1.1/24）向组播组 225.1.1.1 ～ 225.1.1.9 发送组播数据。HostA 能够收到 Source 发出的组播数据。在 RouterE 上查看 PIM 路由表的概要信息。

```
<Huawei> display pim routing-table brief
  VPN-Instance: public net
 Total 9 (*, G) entry; 9 (S, G) entries

  00001.(*, 225.1.1.1)
       Upstream interface:GE4/0/0
       Number of downstream:1
       Number of receive vrf:0
  00002.(10.110.1.1, 225.1.1.1)
       Upstream interface:GE4/0/0
       Number of downstream:1
       Number of receive vrf:0
  00003.(*, 225.1.1.2)
       Upstream interface:GE3/0/0
       Number of downstream:1
       Number of receive vrf:0
  00004.(10.110.1.1, 225.1.1.2)
       Upstream interface:GE3/0/0
       Number of downstream:1
       Number of receive vrf:0
  00005.(*, 225.1.1.3)
       Upstream interface:GE1/0/0
       Number of downstream:1
       Number of receive vrf:0
  00006.(10.110.1.1, 225.1.1.3)
       Upstream interface:GE1/0/0
       Number of downstream:1
       Number of receive vrf:0
  00007.(*, 225.1.1.4)
       Upstream interface:GE1/0/0
       Number of downstream:1
       Number of receive vrf:0
  00008.(10.110.1.1, 225.1.1.4)
       Upstream interface:GE1/0/0
       Number of downstream:1
       Number of receive vrf:0
  00009.(*, 225.1.1.5)
       Upstream interface:GE1/0/0
       Number of downstream:1
       Number of receive vrf:0
  00010.(10.110.1.1, 225.1.1.5)
       Upstream interface:GE1/0/0
       Number of downstream:1
       Number of receive vrf:0
  00011.(*, 225.1.1.6)
       Upstream interface:GE1/0/0
       Number of downstream:1
       Number of receive vrf:0
  00012.(10.110.1.1, 225.1.1.6)
       Upstream interface:GE3/0/0
       Number of downstream:1
       Number of receive vrf:0
  00013.(*, 225.1.1.7)
       Upstream interface:GE1/0/0
       Number of downstream:1
       Number of receive vrf:0
  00014.(10.110.1.1, 225.1.1.7)
       Upstream interface:GE1/0/0
       Number of downstream:1
       Number of receive vrf:0
```

```
00015.(*, 225.1.1.8)
     Upstream interface:GE1/0/0
     Number of downstream:1
     Number of receive vrf:0
00016.(10.110.1.1, 225.1.1.8)
     Upstream interface:GE3/0/0
     Number of downstream:1
     Number of receive vrf:0
00017.(*, 225.1.1.9)
     Upstream interface:GE1/0/0
     Number of downstream:1
     Number of receive vrf:0
00018.(10.110.1.1, 225.1.1.9)
     Upstream interface:GE1/0/0
     Number of downstream:1
     Number of receive vrf:0
```

已存在的(*,G)和(S,G)表项的上游接口没有变化。由于 GigabitEthernet1/0/0 的组播负载分担权值大于 GigabitEthernet3/0/0，则以 GigabitEthernet1/0/0 为上游接口的新增表项数量大于 GigabitEthernet3/0/0。GigabitEthernet4/0/0 的组播负载分担权值为 0，没有参与新增表项的组播负载分担。

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 multicast routing-enable
#
isis 1
 network-entity 10.0000.0000.0001.00
#
interface GigabitEthernet1/0/0
 ip address 10.110.1.2 255.255.255.0
 isis enable 1
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.1.1 255.255.255.0
 isis enable 1
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 192.168.2.1 255.255.255.0
 isis enable 1
 pim sm
#
interface GigabitEthernet4/0/0
 ip address 192.168.3.1 255.255.255.0
 isis enable 1
 pim sm
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
 pim sm
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 multicast routing-enable
#
isis 1
 network-entity 10.0000.0000.0002.00
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
 isis enable 1
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.4.1 255.255.255.0
 isis enable 1
 pim sm
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
 multicast routing-enable
#
isis 1
 network-entity 10.0000.0000.0003.00
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.2 255.255.255.0
 isis enable 1
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.5.1 255.255.255.0
 isis enable 1
 pim sm
#
return
```

- RouterD 的配置文件

```
#
 sysname RouterD
#
 multicast routing-enable
#
isis 1
 network-entity 10.0000.0000.0004.00
#
interface GigabitEthernet1/0/0
 ip address 192.168.3.2 255.255.255.0
 isis enable 1
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.6.1 255.255.255.0
 isis enable 1
 pim sm
#
return
```

- RouterE 的配置文件

```
#
 sysname RouterE
#
 multicast routing-enable
 multicast load-splitting stable-preferred
#
```

```
isis 1
 network-entity 10.0000.0000.0005.00
#
interface GigabitEthernet1/0/0
 ip address 192.168.4.2 255.255.255.0
 isis enable 1
 pim sm
 multicast load-splitting weight 2
#
interface GigabitEthernet2/0/0
 ip address 10.110.2.2 255.255.255.0
 isis enable 1
 pim sm
 igmp static-group 225.1.1.1 inc-step-mask 0.0.0.1 number 3
 igmp static-group 225.1.1.4 inc-step-mask 0.0.0.1 number 6
#
interface GigabitEthernet3/0/0
 ip address 192.168.5.2 255.255.255.0
 isis enable 1
 pim sm
#
interface GigabitEthernet4/0/0
 ip address 192.168.6.2 255.255.255.0
 isis enable 1
 pim sm
 multicast load-splitting weight 0
#
return
```