2 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，可以实现组播设备对本地网络组成员的管理。

2.1 IGMP简介
介绍IGMP的定义和目的。

2.2 IGMP原理描述
介绍IGMP的版本以及各版本的工作原理。

2.3 IGMP应用场景
介绍IGMP的应用场景。

2.4 配置IGMP任务概览
介绍IGMP的配置任务概览。

2.5 IGMP配置注意事项
介绍配置IGMP的注意事项。

2.6 IGMP缺省配置
介绍缺省情况下，IGMP的配置信息。

2.7 配置IGMP基本功能
通过在与用户网段相连的组播路由器接口上配置IGMP基本功能，可以使成员主机接入IPv4组播网络、收到IPv4组播报文。

2.8 调整IGMP性能
配置IGMP基本功能后，缺省情况下组播路由器可以正常工作。也可以根据安全性和网络性能优化的要求，适当调整相关参数，改善IGMP性能。

2.9 配置IGMP SSM Mapping
为了使运行IGMPv1或IGMPv2的主机能够使用SSM服务，可以在组播路由器上配置IGMP SSM Mapping功能，向运行IGMPv1或IGMPv2的成员提供SSM服务。

2.10 配置IGMP Limit
IGMP Limit提供了对组成员关系的个数限制功能。

2.11 配置IGMP Proxy功能
在一些简单的树形网络拓扑中，与成员主机网段直连的组播设备上不需要运行复杂的组播路由协议（如PIM）。可以在这些设备上配置IGMP Proxy功能，使其代理上游接

入设备和下游成员主机的功能，从而有效地节约网络带宽，减轻接入设备的处理压力。

2.12 维护IGMP
IGMP的维护包括：清除IGMP的组信息、清除IGMP报文统计信息、监控IGMP运行状况。

2.13 IGMP配置举例
针对如何在组播网络中配置IGMP基本功能、静态加入组、IGMP SSM Mapping、IGMP Limit、IGMP Proxy，分别提供配置举例。

2.14 IGMP常见配置错误
介绍了常见的配置错误的故障现象以及处理步骤。

2.15 IGMP参考信息
介绍IGMP的相关RFC清单。

2.1 IGMP 简介

介绍IGMP的定义和目的。

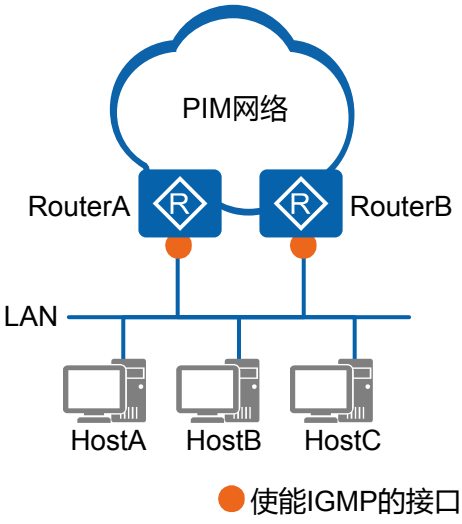
定义

IGMP是Internet Group Management Protocol的简称，又被称为互联网组管理协议，是TCP/IP协议族中负责IPv4组播成员管理的协议。IGMP用来在接收者主机和与其直接相邻的组播路由器之间建立和维护组播组成员关系。IGMP通过在接收者主机和组播路由器之间交互IGMP报文实现组成员管理功能，IGMP报文封装在IP报文中。

目的

IP组播通信的特点是报文从一个源发出，被转发到一组特定的接收者。但在组播通信模型中，发送者不关注接收者的位置信息，只是将数据发送到约定的目的组播地址。要使组播报文最终能够到达接收者，需要某种机制使连接接收者网段的组播路由器能够了解到该网段存在哪些组播接收者，同时保证接收者可以加入相应的组播组中。IGMP就是用来在接收者主机和与其所在网段直接相邻的组播路由器之间建立、维护组播组成员关系的协议。IGMP在组播网络中的部署位置如图2-1所示。

图 2-1 IGMP 在组播网络中的部署位置



2.2 IGMP 原理描述

介绍IGMP的版本以及各版本的工作原理。

2.2.1 IGMP 版本

到目前为止，IGMP有三个版本：

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

IGMPv1中定义了基本的组成员查询和报告过程，IGMPv2在此基础上添加了查询器选举和组成员离开的机制，IGMPv3中增加的主要功能是成员可以指定接收或指定不接收某些组播源的报文。三个版本在演进过程中对协议报文的处理是向前兼容的，因此尽管各个版本的协议报文格式不同，但是运行IGMP高版本的路由器可以识别低版本的IGMP报文。

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IGMP SSM Mapping技术的支持才可以应用于SSM模型。有关ASM和SSM模型的介绍，请参见**组播服务模型**。

IGMP三个版本的比较如**表2-1**所示。

表 2-1 IGMP 三个版本的比较

项目	IGMPv1	IGMPv2	IGMPv3
查询器选举方式	依靠组播路由协议PIM选举	同网段组播路由器之间竞争选举	同网段组播路由器之间竞争选举
普遍组查询报文	支持	支持	支持
成员报告报文	支持	支持	支持
特定组查询报文	不支持	支持	支持
成员离开报文	不支持	支持	没有定义专门的成员离开报文，成员离开通过特定类型的报告报文来传达
特定源组查询报文	不支持	不支持	支持
指定组播源	不支持	不支持	支持
可识别报文协议版本	IGMPv1	IGMPv1、IGMPv2	IGMPv1、IGMPv2、IGMPv3
ASM模型	支持	支持	支持

项目	IGMPv1	IGMPv2	IGMPv3
SSM模型	需要IGMP SSM Mapping技术支持	需要IGMP SSM Mapping技术支持	支持

2.2.2 IGMPv1 工作原理

IGMPv1 报文

IGMPv1包括两种类型的报文：

- 普遍组查询报文（General Query）：查询器向共享网络上所有主机和路由器发送的查询报文，用于了解哪些组播组存在成员。
- 成员报告报文（Report）：主机向查询器发送的报告报文，用于申请加入某个组播组或者应答查询报文。

IGMPv1报文的格式如图2-2所示，其中各个字段的说明见表2-2。

图 2-2 IGMPv1 报文格式

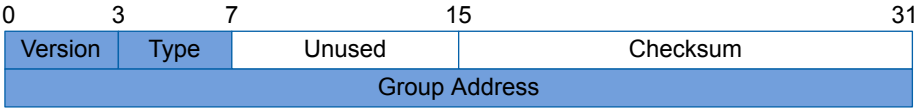


表 2-2 IGMPv1 报文字段说明

字段	说明
Version	IGMP版本，值为1。
Type	报文类型。该字段有以下两种取值： ● 0x1：表示普遍组查询报文。 ● 0x2：表示成员报告报文。
Unused	在IGMPv1中，该字段在发送时被设为0，并在接收时被忽略。
Checksum	IGMP报文的校验和。校验和是IGMP报文长度（即IP报文的整个有效负载）的16位检测，表示IGMP信息补码之和的补码。Checksum字段在进行校验计算时设为0。当发送报文时，必须计算校验和并插入到Checksum字段中去。当接收报文时，校验和必须在处理该报文之前进行检验。
Group Address	组播组地址。在普遍组查询报文中，该字段设为0；在成员报告报文中，该字段为成员加入的组播组地址。

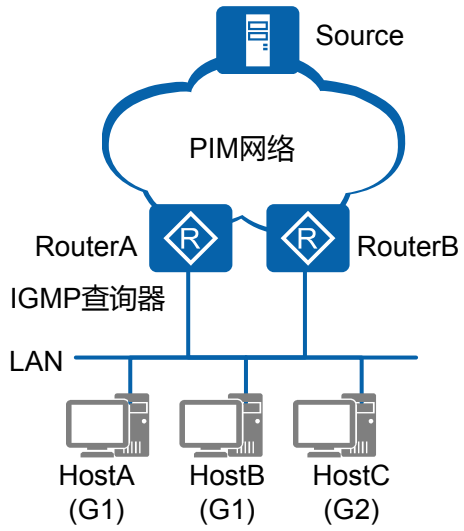
IGMPv1 工作机制

IGMPv1协议主要基于查询和响应机制完成组播组管理。当一个网段内有多个组播路由器时，由于它们都可以接收到主机发送的成员报告报文，因此只需要选取其中一台组播路由器发送查询报文就足够了，该组播路由器称为IGMP查询器（Querier）。在IGMPv1中，由组播路由协议PIM选举出唯一的组播信息转发者（Assert Winner或DR）作为IGMPv1的查询器，负责该网段的组成员关系查询。

有关Assert和DR的介绍，请参见**4.2.2 PIM-DM**和**4.2.3 PIM-SM（ASM模型）**。

下面以**图2-3**所示组网为例，介绍IGMPv1的工作机制。如**图2-3**所示，组播网络中RouterA和RouterB连接主机网段，RouterA为IGMP查询器，在主机网段上有HostA、HostB、HostC三个接收者。HostA和HostB想要接收发往组播组G1的数据，HostC想要接收发往组播组G2的数据。

图 2-3 组播网络示意图

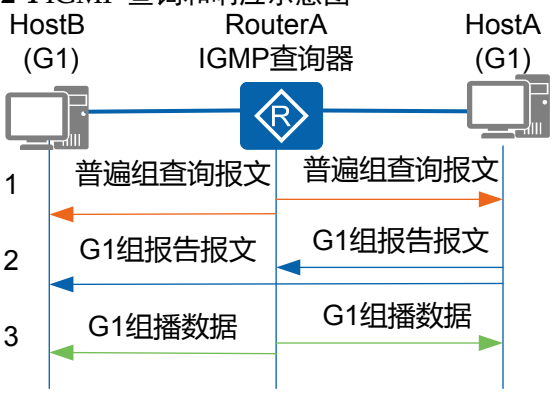


IGMPv1的工作机制可以分为**普遍组查询和响应机制**、**新组成员加入机制**和**组成员离开机制**三个方面。

普遍组查询和响应机制

通过普遍组查询和响应，IGMP查询器可以了解到该网段内哪些组播组存在成员。

图 2-4 IGMP 查询和响应示意图



如图2-4所示，普遍组查询和响应过程如下：

1. IGMP查询器发送目的地址为224.0.0.1（表示同一网段内所有主机和路由器）的普遍组查询报文；收到该查询报文的组成员启动定时器。

   普遍组查询报文是周期性发送的，发送周期可以通过命令配置，缺省情况下每隔60秒发送一次。HostA和HostB是组播组G1的成员，则在本地启动定时器Timer-G1。缺省情况下，定时器的范围为0～10秒之间的随机值。

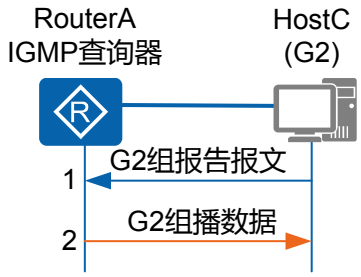
2. 第一个定时器超时的组成员发送针对该组的报告报文。

   假设HostA上的Timer-G1首先超时，HostA向该网段发送目的地址为G1的报告报文。也想加入组G1的HostB收到此报告报文，则停止定时器Timer-G1，不再发送针对G1的报告报文。这样报告报文被抑制，可以减少网段上的流量。

3. IGMP查询器接收到HostA的报告报文后，了解到本网段内存在组播组G1的成员，则由组播路由协议生成（*，G1）组播转发表项，“*”代表任意组播源。网络中一旦有组播组G1的数据到达路由器，将向该网段转发。

新组成员加入机制

图 2-5 新组成员加入示意图



如图2-5所示，主机HostC加入组播组G2的过程如下：

1. 主机HostC不等待普遍组查询报文的到来，主动发送针对G2的报告报文以声明加入。
2. IGMP查询器接收到HostC的报告报文后，了解到本网段内出现了组播组G2的成员，则生成组播转发项（*，G2）。网络中一旦有G2的数据到达路由器，将向该网段转发。

组成员离开机制

IGMPv1没有专门定义离开组的报文。主机离开组播组后，便不会再对普遍组查询报文做出回应。如图2-3所示。

- 假设HostA想要退出组播组G1

  HostA收到IGMP查询器发送的普遍组查询报文时，不再发送针对G1的报告报文。由于网段内还存在G1组成员HostB，HostB会向IGMP查询器发送针对G1的报告报文，因此IGMP查询器感知不到HostA的离开。

- 假设HostC想要退出组播组G2

  HostC收到IGMP查询器发送的普遍组查询报文时，不再发送针对G2的报告报文。由于网段内不存在组G2的其他成员，IGMP查询器不会收到G2组成员的报告报文，则在一定时间（缺省值为130秒）后，删除G2所对应的组播转发表项。

2.2.3 IGMPv2 的变化

IGMPv2的工作机制与IGMPv1基本相同，最大的不同之处在于IGMPv2增加了离开组机制。成员主机离开组播组时，会主动发送成员离开报文通知IGMP查询器；IGMP查询器收到成员离开报文后，会连续发送特定组查询报文，询问该组播组是否还存在组成员。如果在一段时间内没有收到成员主机发送的报告报文，IGMP查询器将不再维护该组的组成员关系。IGMPv2可以使IGMP查询器及时了解到网段内哪些组播组已不存在成员，从而及时更新组成员关系，减少网络中冗余的组播流量。

IGMPv2 报文

与IGMPv1相比，IGMPv2的变化如下：

- 除了普遍组查询报文和成员报告报文之外，IGMPv2新增了两种报文：
  - 成员离开报文（Leave）：成员离开组播组时主动向查询器发送的报文，用于宣告自己离开了某个组播组。
  - 特定组查询报文（Group-Specific Query）：查询器向共享网段内指定组播组发送的查询报文，用于查询该组播组是否存在成员。
- IGMPv2对普遍组查询报文格式也做了改进，添加了最大响应时间（Max Response Time）字段。此字段取值可以通过命令配置，用于控制成员对于查询报文的响应速度。

IGMPv2报文的格式如图2-6所示，其中各个字段的说明见表2-3。

图 2-6 IGMPv2 报文格式

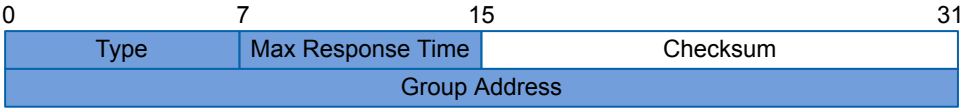


表 2-3 IGMPv2 报文字段说明

字段	说明
Type	报文类型。该字段有以下四种取值： ● 0x11:表示查询报文。IGMPv2的查询报文包括普遍组查询报文和特定组查询报文两类。 ● 0x12:表示IGMPv1成员报告报文。 ● 0x16:表示IGMPv2成员报告报文。 ● 0x17:表示成员离开报文。
Max Response Time	最大响应时间。成员主机在收到IGMP查询器发送的普遍组查询报文后，需要在最大响应时间内做出回应。该字段仅在IGMP查询报文中有效。
Checksum	IGMP报文的校验和。校验和是IGMP报文长度（即IP报文的整个有效负载）的16位检测，表示IGMP信息补码之和的补码。Checksum字段在进行校验计算时设为0。当发送报文时，必须计算校验和并插入到Checksum字段中去。当接收报文时，校验和必须在处理该报文之前进行检验。

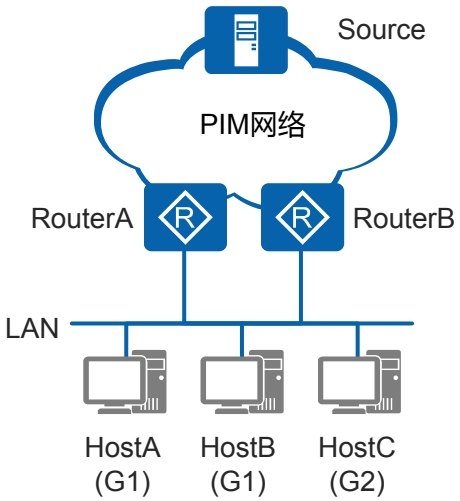
字段	说明
Group Address	组播组地址。 ● 在普遍组查询报文中，该字段设为0。 ● 在特定组查询报文中，该字段为要查询的组播组地址。 ● 在成员报告报文和离开报文中，该字段为成员要加入或离开的组播组地址。

IGMPv2 工作机制

在工作机制上，与IGMPv1相比，IGMPv2增加了查询器选举和离开组机制。

下面以图2-7所示组网为例，介绍IGMPv2的工作机制。如图2-7所示，组播网络中RouterA和RouterB连接主机网段，在主机网段上有HostA、HostB、HostC三个接收者。假设HostA和HostB想要接收发往组播组G1的数据，HostC想要接收发往组播组G2的数据。

图 2-7 组播网络示意图

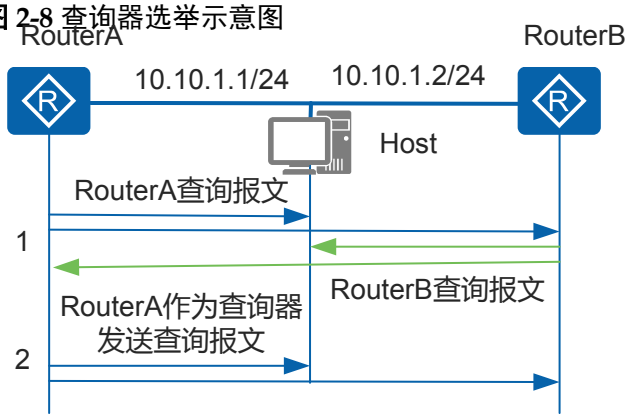


查询器选举机制、离开组机制的过程如下。

查询器选举机制

IGMPv2使用独立的查询器选举机制，当共享网段上存在多个组播路由器时，IP地址最小的路由器成为查询器。

图 2-8 查询器选举示意图



如图2-8所示，在IGMPv2中，查询器的选举过程如下：

1. 最初，所有运行IGMPv2的组播路由器（RouterA和RouterB）都认为自己是查询器，向本网段内的所有主机和组播路由器发送普遍组查询报文。

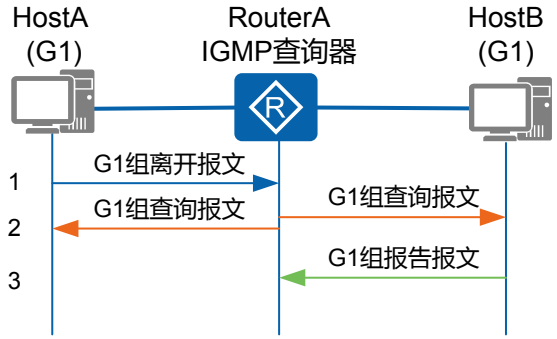
   RouterA和RouterB在收到对方发送的普遍组查询报文后，将报文的源IP地址与自己的接口地址作比较。通过比较，IP地址最小的组播路由器将成为查询器，其他组播路由器成为非查询器（Non-Querier）。如图2-8所示，RouterA的接口地址小于RouterB，则RouterA当选为查询器，RouterB为非查询器。

2. 此后，将由IGMP查询器（RouterA）向本网段内的所有主机和其他组播路由器发送普遍组查询报文，而非查询器（RouterB）则不再发送普遍组查询报文。

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

离开组机制

图 2-9 离开组示意图



如图2-9所示，在IGMPv2中，主机HostA离开组播组G1的过程如下：

1. HostA向本地网段内的所有组播路由器（目的地址为224.0.0.2）发送针对组G1的离开报文。
2. 查询器收到离开报文，会发送针对组G1的特定组查询报文。发送间隔和发送次数可以通过命令配置，缺省情况下每隔1秒发送一次，共发送两次。同时查询器启动组成员关系定时器（Timer-Membership=发送间隔x发送次数）。

3. 该网段内还存在组G1的其他成员（如图2-9所示的HostB），这些成员（HostB）在收到查询器发送的特定组查询报文后，会立即发送针对组G1的报告报文。查询器收到针对组G1的报告报文后将继续维护该组成员关系。

   如果该网段内不存在组G1的其他成员，查询器将不会收到针对组G1的报告报文。在Timer-Membership超时后，查询器将删除（*，G1）对应的IGMP组表项。当有组G1的组播数据到达查询器时，查询器将不会向下游转发。

2.2.4 IGMPv3 的变化

IGMPv3主要是为了配合SSM（Source-Specific Multicast）模型发展起来的，提供了在报文中携带组播源信息的能力，即主机可以对组播源进行选择。

IGMPv3 报文

与IGMPv2相比，IGMPv3报文的变化如下：

- IGMPv3报文包含两大类：查询报文和成员报告报文。IGMPv3没有定义专门的成员离开报文，成员离开通过特定类型的报告报文来传达。
- 查询报文中不仅包含普遍组查询报文和特定组查询报文，还新增了特定源组查询报文（Group-and-Source-Specific Query）。该报文由查询器向共享网段内特定组播组成员发送，用于查询该组成员是否愿意接收特定源发送的数据。特定源组查询通过在报文中携带一个或多个组播源地址来达到这一目的。
- 成员报告报文不仅包含主机想要加入的组播组，而且包含主机想要接收来自哪些组播源的数据。IGMPv3增加了针对组播源的过滤模式（INCLUDE/EXCLUDE），将组播组与源列表之间的对应关系简单的表示为（G，INCLUDE，(S1、S2...)），表示只接收来自指定组播源S1、S2……发往组G的数据；或（G，EXCLUDE，(S1、S2...)），表示接收除了组播源S1、S2……之外的组播源发给组G的数据。当组播组与组播源列表的对应关系发生了变化，IGMPv3报告报文会将该关系变化存放于组记录（Group Record）字段，发送给IGMP查询器。
- 在IGMPv3中一个成员报告报文可以携带多个组播组信息，而之前的版本一个成员报告只能携带一个组播组。这样在IGMPv3中报文数量大大减少。

IGMPv3查询报文的格式如图2-10所示，其中各个字段的说明见表2-4。

图 2-10 IGMPv3 查询报文格式

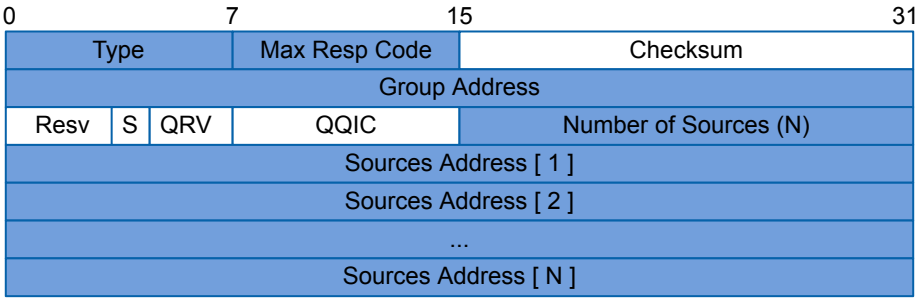


表 2-4 IGMPv3 查询报文字段说明

字段	说明
Type	报文类型，取值为0x11。

字段	说明
Max Response Code	最大响应时间。成员主机在收到IGMP查询器发送的普遍组查询报文后，需要在最大响应时间内做出回应。
Checksum	IGMP报文的校验和。校验和是IGMP报文长度（即IP报文的整个有效负载）的16位检测，表示IGMP信息补码之和的补码。Checksum字段在进行校验计算时设为0。当发送报文时，必须计算校验和并插入到Checksum字段中去。当接收报文时，校验和必须在处理该报文之前进行检验。
Group Address	组播组地址。在普遍组查询报文中，该字段设为0；在特定组查询报文和特定源组查询报文中，该字段为要查询的组播组地址。
Resv	保留字段。发送报文时该字段设为0；接收报文时，对该字段不做处理。
S	该比特位为1时，所有收到此查询报文的其他路由器不启动定时器刷新过程，但是此查询报文并不抑制查询器选举过程和路由器的主机侧处理过程。
QRV	如果该字段非0，则表示查询器的健壮系数（Robustness Variable）。如果该字段为0，则表示查询器的健壮系数大于7。路由器接收到查询报文时，如果发现该字段非0，则将自己的健壮系数调整为该字段的值；如果发现该字段为0，则不做处理。
QQIC	IGMP查询器的查询间隔，单位为秒。非查询器收到查询报文时，如果发现该字段非0，则将自己的查询间隔参数调整为该字段的值；如果发现该字段为0，则不做处理。
Number of Sources	报文中包含的组播源的数量。对于普遍组查询报文和特定组查询报文，该字段为0；对于特定源组查询报文，该字段非0。此参数的大小受到所在网络MTU大小的限制。
Source Address	组播源地址，其数量受到Number of Sources字段值大小的限制。

IGMPv3成员报告报文的格式如图2-11所示，其中各个字段的说明见表2-5。

图 2-11 IGMPv3 成员报告报文格式

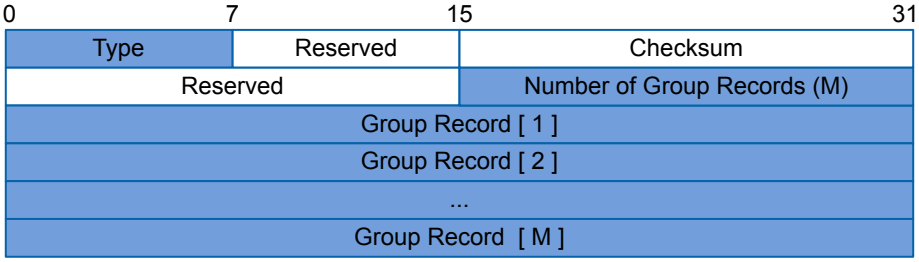


表 2-5 IGMPv3 成员报告报文字段说明

字段	说明
Type	报文类型，取值为0x22。
Reserved	保留字段。发送报文时该字段设为0；接收报文时，对该字段不做处理。
Checksum	IGMP报文的校验和。校验和是IGMP报文长度（即IP报文的整个有效负载）的16位检测，表示IGMP信息补码之和的补码。Checksum字段在进行校验计算时设为0。当发送报文时，必须计算校验和并插入到Checksum字段中去。当接收报文时，校验和必须在处理该报文之前进行检验。
Number of Group Records	报文中包含的组记录的数量。
Group Record	组记录。Group Record字段的格式如图2-12所示，解释如表2-6所示。

图 2-12 Group Record 字段格式

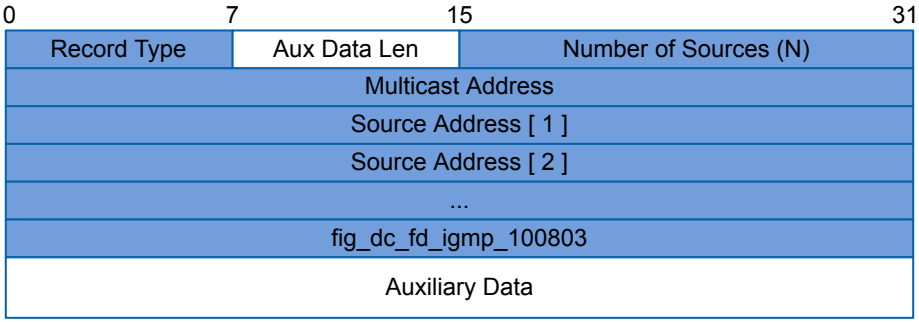


表 2-6 Group Record 字段说明

字段	说明
Record Type	组记录的类型。共分为三大类。 ● 当前状态报告。用于对查询报文进行响应，通告自己目前的状态，共两种：一种是MODE_IS_INCLUDE，表示接收源地址列表包含的源发往该组的组播数据。如果指定源地址列表为空，该报文无效；另一种是MODE_IS_EXCLUDE，表示不接收源地址列表包含的源发往该组的组播数据。 ● 过滤模式改变报告。当组和源的关系在INCLUDE和EXCLUDE之间切换时，会通告过滤模式发生变化，共两种：一种是CHANGE_TO_INCLUDE_MODE，表示过滤模式由EXCLUDE转换到INCLUDE，接收源地址列表包含的新组播源发往该组播组的数据。如果指定源地址列表为空，主机将离开组播组；另一种是CHANGE_TO_EXCLUDE_MODE，表示过滤模式由INCLUDE转换到EXCLUDE，拒绝源地址列表包含的新组播源发往该组的组播数据。 ● 源列表改变报告。当指定源发生改变时，会通告源列表发生变化，共两种：一种是ALLOW_NEW_SOURCES，表示在现有的基础上，需要接收源地址列表包含的组播源发往该组播组的组播数据。如果当前对应关系为INCLUDE，则向现有源列表中添加这些组播源；如果当前对应关系为EXCLUDE，则从现有阻塞源列表中删除这些组播源；另一种是BLOCK_OLD_SOURCES，表示在现有的基础上，不再接收源地址列表包含的组播源发往该组播组的组播数据。如果当前对应关系为INCLUDE，则从现有源列表中删除这些组播源；如果当前对应关系为EXCLUDE，则向现有源列表中添加这些组播源。
Aux Data Len	辅助数据长度。在IGMPv3的报告报文中，不存在辅助数据字段，该字段设为0。
Number of Sources	本记录中包含的源地址数量。
Multicast Address	组播组地址。
Sources Address	组播源地址。
Auxiliary Data	辅助数据。预留给IGMP后续扩展或后续版本。在IGMPv3的报告报文中，不存在辅助数据。关于该字段的详细说明，请参考RFC 3376。

IGMPv3 工作机制

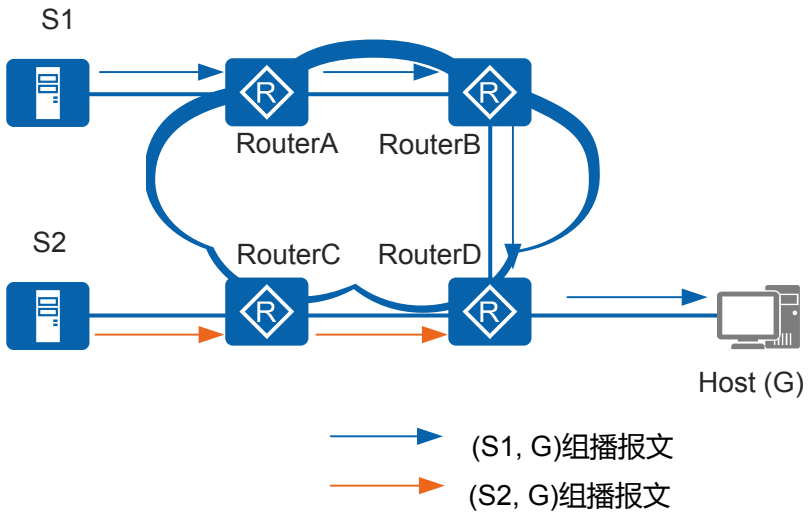
在工作机制上，与IGMPv2相比，IGMPv3增加了主机对组播源的选择能力。

特定源组加入

IGMPv3的成员报告报文的目的地址为224.0.0.22（表示同一网段所有使能IGMPv3的路由器）。通过在报告报文中携带组记录，主机在加入组播组的同时，能够明确要求接

收或不接收特定组播源发出的组播数据。如图2-13所示，网络中存在S1和S2两个组播源，均向组播组G发送组播数据，Host仅希望接收从组播源S1发往组播组G的信息。

图 2-13 特定源组的组播数据流路径



如果Host和组播路由器之间运行的是IGMPv1或IGMPv2，Host加入组播组G时无法对组播源进行选择，无论其是否需要，都会同时接收到来自组播源S1和S2的数据。如果采用IGMPv3，成员主机可以选择仅接收S1组播数据。

- 方法一：Host发送IGMPv3报告（G，INCLUDE，(S1)），仅接收源S1向组播组G发送的数据。
- 方法二：Host发送IGMPv3报告（G，EXCLUDE，(S2)），不接收指定源S2向组播组G发送的数据，从而仅有来自S1的组播数据才能传递到Host。

特定源组查询

当接收到组成员发送的改变组播组与源列表的对应关系的报告时（比如CHANGE_TO_INCLUDE_MODE、CHANGE_TO_EXCLUDE_MODE），IGMP查询器会发送特定源组查询报文。如果组成员希望接收其中任意一个源的组播数据，将反馈报告报文。IGMP查询器根据反馈的组成员报告更新该组对应的源列表。

2.2.5 IGMP SSM Mapping

SSM（Source-Specific Multicast）称为指定源组播，要求路由器能了解成员主机加入组播组时所指定的组播源。如果成员主机上运行IGMPv3，可以在IGMPv3报告报文中直接指定组播源地址。但是某些情况下，成员主机只能运行IGMPv1或IGMPv2，为了使其也能够使用SSM服务，路由器上需要提供IGMP SSM Mapping功能。

IGMP SSM Mapping的机制是：通过在路由器上静态配置SSM地址的映射规则，将IGMPv1和IGMPv2报告报文中的(*, G)信息转化为对应的(G, INCLUDE, (S1, S2...))信息，以提供SSM组播服务。

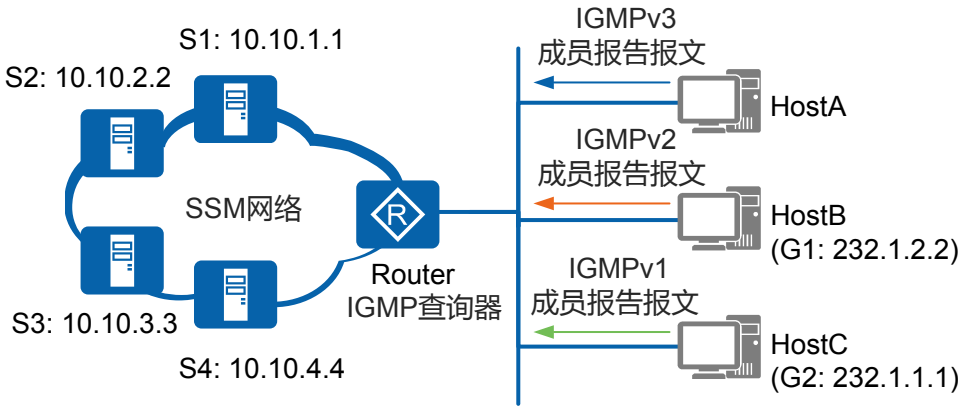
配置了SSM Mapping规则后，当IGMP查询器收到来自成员主机的IGMPv1或IGMPv2报告报文时，首先检查该报文中所携带的组播组地址G，然后根据检查结果的不同分别进行处理。

- 如果G在ASM（Any-Source Multicast）范围内，则只提供ASM服务。

- 如果G在SSM组地址范围内（缺省情况下为232.0.0.0～232.255.255.255）：
  - 如果路由器上没有G对应的SSM Mapping规则，则无法提供SSM服务，丢弃该报文。
  - 如果路由器上有G对应的SSM Mapping规则，则依据规则将报告报文中所包含的(*, G)信息映射为(G, INCLUDE, (S1, S2...))信息，提供SSM服务。

如图2-14所示，SSM网络中HostA运行IGMPv3、HostB运行IGMPv2、HostC运行IGMPv1。HostB和HostC无法升级到IGMPv3，如果要为该网段中的所有主机提供SSM服务，需要在IGMP查询器（Router）上使能IGMP SSM Mapping并配置相应的映射规则。

图 2-14 IGMP SSM Mapping 组网图



假如在Router上配置如下映射关系：

组播组地址	映射的组播源地址
232.0.0.0/8	10.10.1.1
232.1.0.0/16	10.10.2.2
232.1.0.0/16	10.10.3.3
232.1.1.0/24	10.10.4.4

经过映射后，Router收到HostB和HostC的成员报告报文时，首先判断报文携带的组地址是否在SSM范围内，发现在SSM范围内，则根据配置的映射规则生成如下所示的组播表项。如果一个组地址映射了多个源，则生成多个(S, G)表项。

在映射过程中，一个组播组地址只要能在规则中匹配到，都会生成一条相应的表项。因此232.1.1.1有四条表项，232.1.2.2有三条表项。

IGMPv1/IGMPv2报告报文中的组地址	生成的组播表项
232.1.1.1 （来自HostC）	（10.10.1.1，232.1.1.1） （10.10.2.2，232.1.1.1） （10.10.3.3，232.1.1.1） （10.10.4.4，232.1.1.1）
232.1.2.2 （来自HostB）	（10.10.1.1，232.1.2.2） （10.10.2.2，232.1.2.2） （10.10.3.3，232.1.2.2）

说明

IGMP SSM Mapping不处理IGMPv3的报告报文。为了保证同一网段运行任意版本IGMP的主机都能得到SSM服务，需要在与成员主机所在网段相连的组播路由器接口上运行IGMPv3。

2.2.6 IGMP Proxy

如图2-15左图所示，在一些简单的树形网络拓扑中，与用户网段相连的设备RouterB上并不需要运行复杂的组播路由协议（如PIM），而透传主机IGMP报文又会导致RouterA管理太多用户。当网络中存在大量成员主机或大量成员主机频繁加入/离开组播组时，会产生大量的IGMP报告/离开报文，从而给接入设备RouterA带来较大的处理压力。

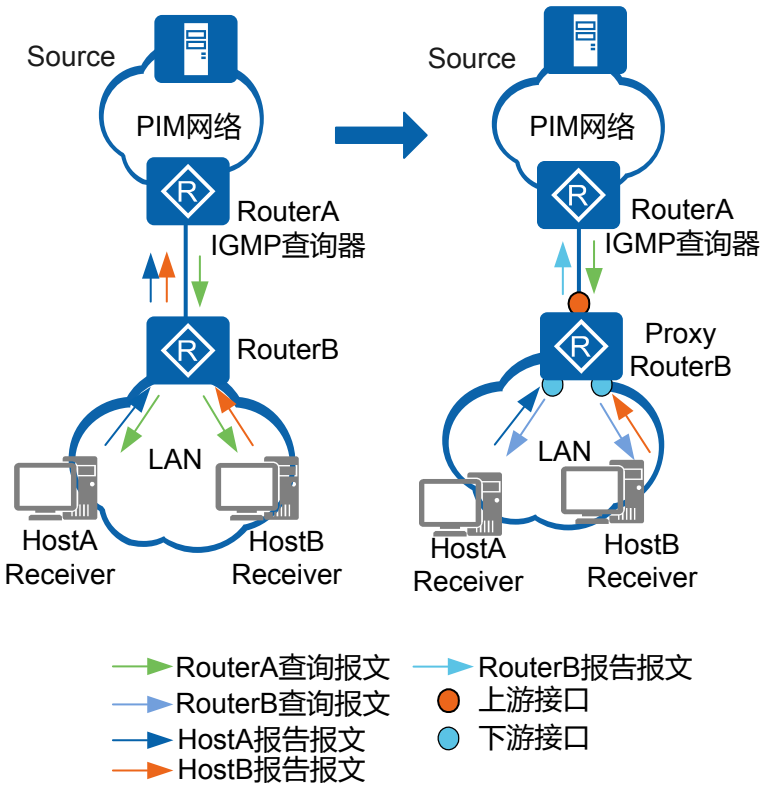
如图2-15右图所示，通过在RouterB上配置IGMP Proxy功能，可以解决以上问题，实现组播报文正常转发同时减轻RouterA的处理压力。

IGMP Proxy，也称为IGMP代理，通常被部署在接入设备（RouterA）和成员主机之间的三层设备上，如图2-15中的RouterB。一方面，IGMP Proxy设备可以收集下游成员主机的IGMP报告/离开报文，将报告/离开报文汇聚后代理下游成员主机统一上送给接入设备；另一方面，IGMP Proxy设备也可以代理IGMP查询器向下游成员主机发送查询报文，维护组成员关系，基于组成员关系进行组播转发。在接入设备RouterA看来，RouterB就是一台主机；在下游成员主机看来，RouterB就是IGMP查询器。

IGMP Proxy中定义了以下两种类型的接口：

- 上游接口：指IGMP代理设备上配置IGMP Proxy功能的接口，该接口执行IGMP代理设备的主机行为，因此也称为主机接口（Host Interface）。
- 下游接口：指IGMP代理设备上配置IGMP功能的接口，该接口执行IGMP代理设备的路由器行为，因此也称为路由器接口（Router Interface）。

图 2-15 IGMP Proxy 组网示意图



IGMP Proxy 工作机制

IGMP代理设备实现的功能主要分为两种：主机行为和路由器行为。

主机行为

主机行为是指IGMP代理设备的上游接口收到查询报文时根据当前组播转发表的状态对查询报文做出响应，或者当组播转发表发生变化时上游接口主动向接入设备发送报告/离开报文。主机行为的工作机制如下：

- IGMP代理设备上游接口收到查询报文时，会根据当前组播转发表的状态对查询报文做出响应。
- IGMP代理设备收到某组播组的报告报文后，会在组播转发表中查找该组播组：
  - 如果没有找到相应的组播组，IGMP代理设备会向接入设备发送针对该组播组的报告报文，并在组播转发表中添加该组播组；
  - 如果找到相应的组播组，IGMP代理设备就不需要向接入设备发送报告报文。
- IGMP代理设备收到某组播组G的离开报文后，会向接收到该离开报文的接口发送一个特定组查询报文，检查该接口下是否还存在组播组G的其他成员：
  - 如果没有其他成员，在组播转发表中将该接口删除，然后判断组播组G是否还有其他接口。如果没有，IGMP代理设备再会向接入设备发送针对该组播组的离开报文；如果有，IGMP代理设备不向接入设备发送针对该组播组的离开报文；
  - 如果有其他成员，IGMP代理设备会继续向该接口转发组播数据。

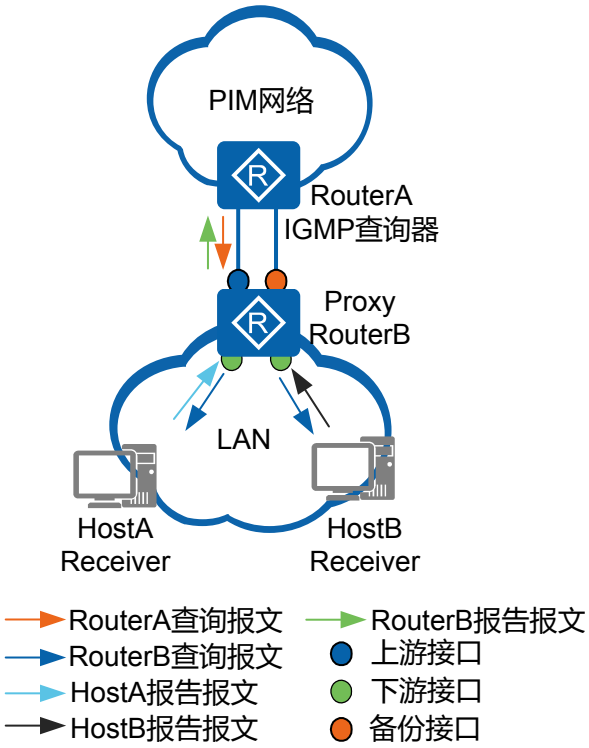
路由器行为

路由器行为是指IGMP代理设备的下游接口通过成员主机加入/离开组播组的信息生成组播转发表项、接收接入设备下发的组播数据并根据组播转发表项的出接口信息向特定的接口转发组播数据。路由器行为的工作机制与IGMP的工作机制一致，请参见**2.2.2 IGMPv1工作原理**、**2.2.3 IGMPv2的变化**、**2.2.4 IGMPv3的变化**。

IGMP Proxy 备份机制

为了提高链路的可靠性，IGMP代理设备的上游接口配置完IGMP Proxy功能后，可以再在IGMP代理设备上配置一个IGMP Proxy备份接口，作为上游接口的备份，如**图2-16**所示。这样，当上游接口所在链路发生故障时，备份链路会自动接管IGMP代理业务，使业务能够自动恢复。

图 2-16 IGMP Proxy 组网示意图



IGMP Proxy本身并没有检测机制，如果组播链路发生了故障，无法保证及时进行主、备链路的切换，可能造成较长时间的组播业务中断。通过IGMP Proxy与NQA联动可以解决此问题。IGMP Proxy与NQA测试例联动是利用NQA测试例检测端到端的链路状态，并根据NQA测试例的检测结果，进行主、备链路的切换，从而避免通信长时间中断。

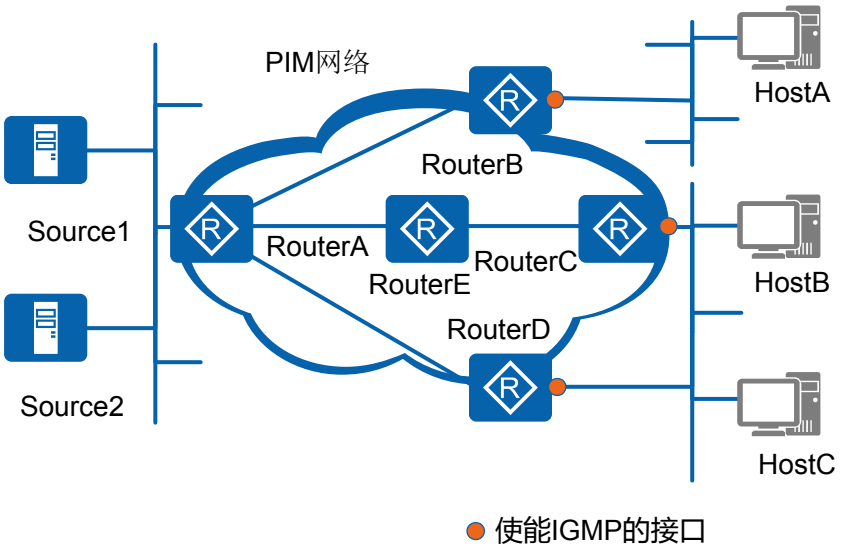
2.3 IGMP 应用场景

介绍IGMP的应用场景。

2.3.1 IGMP 典型应用

IGMP运行在成员主机和与其直接相邻的组播路由器上，负责组播组成员关系的管理和维护。同时，为了将组播源的数据顺利转发到接收者，组播路由器之间需要运行组播路由协议PIM来建立转发路径。图2-17所示为IGMP的典型应用组网图。

图 2-17 IGMP 典型应用组网图



在实际应用中，有如下几种方案。

方案	成员主机	与成员主机相连的路由器接口	网络中的所有路由器
ASM主机动态接入	启用IGMPv1或IGMPv2	启用IGMPv1或IGMPv2	启用PIM-DM或PIM-SM协议
SSM主机动态接入	启用IGMPv3	启用IGMPv3	启用PIM-SM协议
SSM Mapping主机动态接入	启用IGMPv1或IGMPv2	启用IGMPv3，使能IGMP SSM Mapping功能，配置源和组映射关系	启用PIM-SM协议

2.4 配置 IGMP 任务概览

介绍IGMP的配置任务概览。

IGMP的配置任务如表2-7所示。

表 2-7 IGMP 的配置任务概览

场景	描述	对应任务
配置IGMP基本功能	要想使成员主机接入组播网络并接收到组播源的数据，首先需要在与成员主机相连的组播路由器接口上配置IGMP基本功能。	**配置IGMP基本功能**
调整IGMP性能	组播路由器配置了IGMP基本功能后，在缺省配置下可以完成与成员主机之间的IGMP报文交互，实现组成员管理功能。出于安全性或网络性能优化考虑，可以根据需要在组播路由器上调整IGMP性能。	**调整IGMP性能**
配置IGMP SSM Mapping	当成员主机支持IGMPv3时，才可以使用SSM模型提供的在成员端指定组播源的传输服务。有些情况下，成员主机只能运行IGMPv1或IGMPv2。为了使这部分主机也能够使用SSM服务，可以在组播路由器上配置IGMP SSM Mapping功能，向运行IGMPv1或IGMPv2的成员主机提供SSM服务。	**配置IGMP SSM Mapping**
配置IGMP Limit	按照组播协议的规定，组播组成员可以在任意时间、任意位置加入或退出组播组，并且加入的成员总数不受限制。但是当大量用户同时收看多套节目时，需要占用组播设备的大量带宽，可能会造成组播性能下降。为了避免这种情况的发生，组播路由器支持IGMP Limit功能，通过限制全局和接口下的组播组个数，使加入组播组的用户收看更加清晰稳定的节目。	**配置IGMP Limit**

场景	描述	对应任务
配置IGMP Proxy功能	在一些简单的树型网络拓扑中，与用户网段直接相邻的组播路由器上并不需要运行复杂的组播路由协议（如PIM），而透传主机IGMP报文又会导致上游接入设备管理太多用户。此时可以通过在与用户网段直接相邻的组播路由器上配置IGMP Proxy（IGMP代理）功能，使其收集下游用户的IGMP成员报告/离开报文，将成员报告/离开报文汇聚后代理下游主机统一上送给接入设备，并维护组成员关系，基于组成员关系进行组播转发。在上游接入设备看来，配置了IGMP Proxy功能的组播路由器就是一台主机。	配置IGMP Proxy功能
配置IGMP多实例	IGMP多实例是指在VPN实例下配置IGMP协议。路由器通过配置IGMP多实例，就可以完成与私网内成员主机之间的IGMP报文交互，实现私网的组成员管理功能。并且各个VPN实例间配置的IGMP协议互不影响。	IGMP多实例的相关配置，已经包含在本章的所有配置任务中。

2.5 IGMP 配置注意事项

介绍配置IGMP的注意事项。

涉及网元

一个完整的IPv4组播网络涉及以下网元：

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

IGMP组播组，否则上游运行PIM协议的设备无法了解到用户需求，组播转发路径无法正常建立。

- 运行IGMP Snooping的设备：通过侦听上游三层组播设备与组播用户主机之间交互的IGMP报文，生成二层组播转发表项，指导组播数据在二层网络的精确转发。为了避免组播报文二层网络广播，减少带宽浪费，建议在二层设备上配置IGMP Snooping功能。
- 接收者：接收组播数据的组播用户。接收者可以为PC、机顶盒等，但是需要具备相应的组播客户端软件。

License 支持

IGMP是路由器的基本特性，无需获得License许可应用此功能。

特性依赖和限制

在组播路由器上配置IGMP功能时，需要注意：路由器不支持三层组播与透明网桥叠加使用。

2.6 IGMP 缺省配置

介绍缺省情况下，IGMP的配置信息。

表2-8列出了IGMP的缺省配置。

表 2-8 IGMP 缺省配置

参数	缺省值
IP组播路由功能	未使能
IGMP功能	未使能
IGMP版本	IGMPv2
IGMP SSM Mapping	未使能
IGMP普遍组查询间隔	60s
IGMP Proxy	未使能

2.7 配置 IGMP 基本功能

通过在与用户网段相连的组播路由器接口上配置IGMP基本功能，可以使成员主机接入IPv4组播网络、收到IPv4组播报文。

前置任务

在配置IGMP基本功能之前，需配置单播路由协议，使各设备间单播路由可达。

配置流程

2.7.1 使能IGMP功能和2.7.2 配置IGMP版本为必选配置，其他为可选配置，请根据需要选配。

2.7.1 使能 IGMP 功能

背景信息

使能IP组播路由功能是配置一切组播功能的前提。配置组播协议之前，必须先使能IP组播路由功能。

要在组播设备上配置IGMP，首先要在与组成员相连的接口上使能IGMP功能。

操作步骤

- 使能公网实例的IGMP
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**multicast routing-enable**，使能IP组播路由功能。
  缺省情况下，没有使能IP组播路由功能。
  c. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  d. 执行命令**igmp enable**，使能IGMP功能。
  缺省情况下，接口上未使能IGMP功能。
- 使能VPN实例的IGMP

  使能VPN实例的IGMP之前，应该已经创建好VPN实例。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**ip vpn-instance** *vpn-instance-name*，进入VPN实例视图。
  c. 执行命令**multicast routing-enable**，使能IP组播路由功能。
  缺省情况下，没有使能IP组播路由功能。
  d. 执行命令**quit**，退回系统视图。
  e. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  f. 执行命令**ip binding vpn-instance** *vpn-instance-name*，将接口与VPN实例进行关联。
  缺省情况下，接口不与任何VPN实例绑定，属于公网接口。
  g. 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

2.7.2 配置 IGMP 版本

背景信息

运行高版本IGMP的组播路由器可以识别低版本的IGMP报文，但是运行低版本IGMP的组播路由器不能识别高版本的IGMP报文。为了保证IGMP的正常运行，建议在组播路由器上配置和成员主机相同或高于成员主机的IGMP版本。

如果在主机侧共享网段上有多个组播路由器，为了防止因组播路由器上配置的IGMP协议版本不同而导致的IGMP功能无法正常运行，必须在所有组播路由器与组成员相连的接口上配置相同的IGMP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**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IGMP版本。

缺省情况下，接口使能IGMP后运行IGMPv2。

----结束

2.7.3 （可选）配置静态组播组

背景信息

在某些特殊的应用场景中，比如：

- 网络中存在稳定的组播组成员；
- 主机无法发送报告报文，但是又需要将组播数据转发到该网段。

为了实现组播数据的快速、稳定转发，或者将组播数据引流到接口，可以在组播路由器的用户侧接口上配置静态组播组。在接口上配置静态组播组后，组播路由器就认为此接口网段上一直存在该组播组的成员，从而转发该组的组播数据。

当成员主机无法解析组播ping报文并作出回应时，可以在组播路由器的用户侧接口上配置组播ping功能。这样，接口除了正常接收组播数据之外，还可以对收到的组播ping报文作出回应，从而使定位问题更加灵活、方便。

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*]，配置接口静态加入组播组或组播源组。

缺省情况下，接口未配置任何静态组播组。

说明

如果在Loopback接口上配置静态加入组播组或组播源组，组播路由器将组播数据引入后不会立即转发出去，当有用户点播到该组数据才转发，从而减少网络流量。其他支持IGMP的接口会立即转发。比如，对于用户可能点播而尚未点播的组播组，可以在Loopback接口上配置；对于某些存在稳定成员的组播组，可以在与用户网段相连的接口上配置。

步骤4 （可选）执行命令**igmp static-group** *group-address* [**source** *source-address*] **mping-echo**，配置接口可以对收到的组播ping报文作出回应。

缺省情况下，接口不回应收到的组播ping报文。

----结束

2.7.4 （可选）配置接口加入的组播组范围

背景信息

为了限定接口所在网段的成员主机加入的组播组范围，可以配置ACL规则，对收到的成员报告报文进行过滤，只对该规则允许的组播组维护组成员关系。ACL的配置方法，请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列企业路由器 配置指南-安全》中的“ACL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**]，配置接口下的成员主机可以加入的组播组范围。

缺省情况下，接口可以加入任何组播组。

说明

在定义ACL的**rule**时，通过**permit**参数仅允许接口下成员主机可以加入指定地址范围的组播组。如果ACL未定义**rule**，则禁止接口下成员主机加入所有组播组。

----结束

2.7.5 检查配置 IGMP 基本功能的结果

背景信息

IGMP基本功能配置成功后，在任意视图下执行下面的命令，可以查看接口上的IGMP配置和运行信息、组成员信息。

操作步骤

- 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]，查看接口上的IGMP配置和运行信息。
- 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address* | **interface** *interface-type interface-number*]* [**verbose**]，查看动态加入IGMP组播组的成员信息。
- 执行以下命令，查看静态IGMP组播组的成员信息。
  - 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] **static** [**up** | **down**] [**verbose**]，查看状态是Up或Down并且静态加入组播组的接口信息。
  - 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] **static interface-number**，查看加入IGMP静态组播组的接口数量。
  - 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] **interface** *interface-type interface-number* **static** [**verbose**]，查看指定接口上静态加入的组播组信息。

- 执行命令**display igmp [vpn-instance** *vpn-instance-name* **| all-instance] group static interface** *interface-type interface-number* **entry-number**，查看指定接口上加入的IGMP静态组播组数量。

----结束

2.8 调整 IGMP 性能

配置IGMP基本功能后，缺省情况下组播路由器可以正常工作。也可以根据安全性和网络性能优化的要求，适当调整相关参数，改善IGMP性能。

前置任务

2.7 配置IGMP基本功能

配置流程

以下任务是并列的、可选的，可以根据需要选择执行下面的配置任务。

2.8.1 配置 Router-Alert 选项

背景信息

通常情况下，网络设备收到报文时，只有目的IP地址为本设备接口地址的报文才会上送给相应的协议模块处理。如果协议报文的目的地址不是本设备的接口地址，比如IGMP协议报文，由于其目的地址为组播地址，这种情况下就无法上送给IGMP协议模块处理，导致正常的组成员关系不能维护。为了解决此类问题，Router-Alert选项应运而生。如果IP报文头中携带Router-Alert选项，设备在接收到此类报文后，会直接上送给相应的协议模块处理，而不检查目的地址。

出于兼容性考虑，当前路由器在收到IGMP报文后，无论其IP报文头是否包含Router-Alert选项，缺省情况下都会上送给IGMP协议模块处理。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，也可以配置路由器丢弃未携带Router-Alert选项的IGMP报文。

路由器在发送IGMP报文时，也可以选择是否需要携带Router-Alert选项。缺省情况下，组播路由器发送的IGMP报文中携带Router-Alert选项。当需要与不支持Router-Alert选项的设备互通时，可以配置路由器在发送IGMP报文时不包含Router-Alert选项。

说明

配置Router-Alert选项同时支持全局配置（即IGMP视图）和接口配置，生效原则如下：

- 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。接口视图下没有配置时，IGMP视图下配置的值有效。
- 如果IGMP视图下配置非缺省值，则接口视图下配置的缺省值无效。

操作步骤

- 配置全局Router-Alert选项
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**igmp [vpn-instance** *vpn-instance-name* **]**，进入IGMP视图。

c. 执行命令**require-router-alert**，配置设备在收到IGMP报文时检查Router-Alert选项，丢弃不包含Router-Alert选项的IGMP报文。

缺省情况下，设备不检查Router-Alert选项，即处理所有接收到的IGMP报文，包括无Router-Alert选项的IGMP报文。

d. 执行命令**send-router-alert**，配置设备在发送的IGMP报文头中包含Router-Alert选项。

缺省情况下，设备发送的IGMP报文头中包含Router-Alert选项。

- 配置接口下Router-Alert选项

a. 执行命令**system-view**，进入系统视图。

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

c. 执行命令**igmp require-router-alert**，配置接口在收到IGMP报文时检查Router-Alert选项，丢弃不包含Router-Alert选项的IGMP报文。

缺省情况下，接口不检查Router-Alert选项，即处理所有接收到的IGMP报文，包括无Router-Alert选项的IGMP报文。

d. 执行命令**igmp send-router-alert**，配置接口在发送的IGMP报文头中包含Router-Alert选项。

缺省情况下，接口发送的IGMP报文头中包含Router-Alert选项。

----结束

2.8.2 配置 IGMP 查询器参数

背景信息

IGMP通过查询和响应报文维护组成员关系。当同一网段上有多台组播路由器时，由IGMP查询器负责发送IGMP查询报文。IGMP查询器在工作过程中使用了多项参数，当这些参数均为缺省值时，IGMP查询器可以正常工作。同时，为了使组成员关系得到及时的更新维护，避免报文发送过多造成网络拥塞，也可以通过命令行对IGMP查询器的参数进行合理的调整。

表2-9列出了IGMP查询器各参数的说明和缺省值。

表 2-9 IGMP 查询器各参数的说明和缺省值

参数	参数说明	缺省值
IGMP普遍组查询报文的发送时间间隔	查询器周期性的发送普遍组查询报文，维护接口上的组成员关系。本参数定义了查询器发送普遍组查询报文的时间间隔。	60s

参数	参数说明	缺省值
IGMP查询器的健壮系数	查询器的健壮系数是为了弥补可能发生的网络丢包而设置的报文重传次数。 该参数用来规定以下两个值： ● 查询器启动时，发送“健壮系数”次的“普遍组查询报文”。 ● 查询器收到针对某组播组的离开报文时，发送“健壮系数”次的特定组\源组查询报文，询问该组播组是否还存在成员。	2
IGMP普遍组查询报文的最大响应时间	组播组成员接收到一个IGMP普遍组查询报文后，会在最大响应时间内发送Report报文回应IGMP查询器。	10s
其他IGMP查询器的存活时间	如果非查询器在“其他IGMP查询器的存活时间”内收不到查询报文，就认为查询器失效，自动发起查询器选举。	当IGMP普遍组查询报文的发送时间间隔、IGMP查询器健壮系数和IGMP普遍组查询报文的最大响应时间都取缺省值时，其他IGMP查询器的存活时间为125秒
IGMP特定组\源组查询报文的发送时间间隔	当查询器收到主机退出某组播组的离开报文时，会连续发送IGMP特定组\源组查询报文，询问该组播组是否还存在成员。本参数定义了发送报文的时间间隔。	1s

说明

在共享网段内，如果多台设备的用户侧接口都使能了IGMP，应确保设备上配置的查询器参数一致，否则有可能导致IGMP协议无法正常运行。

此项配置同时支持全局配置（即IGMP视图）和接口配置，生效原则如下：

- 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。接口视图下没有配置时，IGMP视图下配置的值有效。
- 如果IGMP视图下配置非缺省值，则接口视图下配置的缺省值无效。

操作步骤

- 配置全局IGMP查询器参数
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**igmp** [**vpn-instance** *vpn-instance-name*]，进入IGMP视图。
  c. 执行命令**timer query** *interval*，配置设备发送IGMP普遍组查询报文的时间间隔。

d. 执行命令**robust-count** *robust-value*，配置IGMP查询器的健壮系数。

e. 执行命令**max-response-time** *interval*，配置IGMP普遍组查询报文的最大响应时间。

f. 执行命令**timer other-querier-present** *interval*，配置其他IGMP查询器的存活时间。

g. 执行命令**lastmember-queryinterval** *interval*，配置设备发送IGMP特定组\源组查询报文的时间间隔。

说明

实际配置中，要确保“IGMP查询报文最大响应时间”<“IGMP普遍组查询报文发送时间间隔”<“其他IGMP查询器存活时间”，否则有可能出现IGMP Report报文响应IGMP查询不及时，导致设备上删除表项。

- 配置接口下IGMP查询器参数

a. 执行命令**system-view**，进入系统视图。

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

c. 执行命令**igmp timer query** *interval*，配置接口发送IGMP普遍组查询报文的时间间隔。

d. 执行命令**igmp robust-count** *robust-value*，配置IGMP查询器的健壮系数。

e. 执行命令**igmp max-response-time** *interval*，配置IGMP普遍组查询报文的最大响应时间。

f. 执行命令**igmp timer other-querier-present** *interval*，配置其他IGMP查询器的存活时间。

g. 执行命令**igmp lastmember-queryinterval** *interval*，配置接口发送IGMP特定组\源组查询报文的时间间隔。

说明

实际配置中，要确保“IGMP查询报文最大响应时间”<“IGMP普遍组查询报文发送时间间隔”<“其他IGMP查询器存活时间”，否则有可能出现IGMP Report报文响应IGMP查询不及时，导致设备上删除表项。

----结束

2.8.3 配置 IGMP 快速离开

背景信息

在某些应用（如ADSL拨号上网）中，IGMP查询器的一个接口下只连接着一台成员主机，当主机在多个组播组间频繁切换（如进行电视选台）时，为了快速响应主机的离开组报文，可以在IGMP查询器上配置IGMP快速离开功能。

在配置了IGMP快速离开功能之后，当查询器收到来自主机的离开报文时，不再发送特定组查询报文，而是直接向上游发送离开通告。这样一方面减小了响应延迟，另一方面也节省了网络带宽。

IGMP快速离开功能仅适用于IGMPv2和IGMPv3。

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 prompt-leave [group-policy** { *acl-number* | **acl-name** *acl-name* }]，配置接口快速离开功能。

缺省情况下，路由器在收到离开报文后会发送特定组查询报文。

说明

在定义ACL的**rule**时，通过**permit**参数仅允许接口下成员主机快速离开指定地址范围的组播组。如果ACL未定义**rule**，则禁止接口下成员主机快速离开所有组播组。

----结束

2.8.4 配置 IGMP On-Demand

背景信息

在标准的IGMP工作机制中，查询器通过周期性发送查询报文并接收成员反馈的报告和离开报文来了解组播组成员信息。当网络中的组成员关系比较稳定时，为了减少IGMP的报文交互数目，降低网络流量，可以在查询器上配置IGMP On-Demand功能。IGMP On-Demand是指查询器根据成员的要求来维护成员关系，不主动发送查询报文去收集成员状态，这样可以减少查询器和成员主机之间的IGMP报文数量。

路由器接口上配置了IGMP On-Demand特性后：

- 接口不再发送IGMP查询报文。
- 收到报告报文后创建组表项，且创建的表项永不超时。
- 收到IGMP离开报文后，立即删除接口上对应的组表项。

IGMP On-Demand只适用于IGMPv2和IGMPv3。

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 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，接口周期性发送查询报文，参与查询器选举。

说明

如果查询器上有动态IGMP组表项存在，请先执行**reset igmp group**命令清除IGMP组表项后再执行**igmp on-demand**命令。

----结束

2.8.5 配置根据源地址过滤 IGMP 报文

背景信息

IGMP运行在成员主机和与主机网段直连的三层组播设备上，组播路由器会对收到的所有IGMP报文进行处理。为了提高安全性，避免网络中其他设备恶意伪造IGMP报文而影响正常的组播业务，可以在路由器与成员主机相连的接口上配置对IGMP报文进行过滤。这里可以过滤的报文包括查询报文、报告/离开报文。

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**igmp query ip-source-policy** { *basic-acl-number* | **acl-name** *acl-name* }，过滤IGMP查询报文。

缺省情况下，路由器不对查询报文进行过滤，即处理所有接收到的查询报文。

说明

在定义ACL的**rule**时，通过**permit**参数配置接口仅接收指定源地址范围的查询报文。如果ACL未定义**rule**，则接口默认过滤掉所有查询报文。

步骤4 执行命令**igmp ip-source-policy** [*basic-acl-number* | **acl-name** *acl-name*]，过滤IGMP报告/离开报文。

缺省情况下，路由器不对IGMP报告/离开报文进行过滤，即处理所有接收到的IGMP报告/离开报文。

如果不配置ACL，路由器对IGMP报告/离开报文的源地址检查的规则如下：

- 如果源地址和接收报文的接口地址在同一网段，或者源地址是0.0.0.0，正常处理该报文。
- 如果源地址和接收报文的接口地址不在同一网段，丢弃该报文。

说明

在定义ACL的**rule**时，通过**permit**参数配置接口仅接收指定源地址范围的IGMP报告/离开报文。如果ACL未定义**rule**，则接口默认过滤掉所有IGMP报告/离开报文。

----结束

2.8.6 检查配置调整 IGMP 性能的结果

背景信息

完成上述操作后，在任意视图下执行以下命令，可以查看调整后的组成员信息、IGMP配置和运行信息。

操作步骤

- 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address* | **interface** *interface-type interface-number*]* [**verbose**]，查看通过主机发送报告报文动态加入的IGMP组播组信息。
- 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]，查看接口上IGMP配置和运行信息。
- 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }]]* [**static**] [**outgoing-interface-number** [*number*]]，查看IGMP路由表信息。

----结束

2.9 配置 IGMP SSM Mapping

为了使运行IGMPv1或IGMPv2的主机能够使用SSM服务，可以在组播路由器上配置IGMP SSM Mapping功能，向运行IGMPv1或IGMPv2的成员提供SSM服务。

前置任务

2.7.1 使能IGMP功能

背景信息

当成员主机支持IGMPv3时，才可以使用SSM模型提供的在成员端指定组播源的传输服务。有些情况下，成员主机只能运行IGMPv1或IGMPv2，为了使这部分主机也能够使用SSM服务，可以在组播路由器上配置IGMP SSM Mapping功能。IGMP SSM Mapping通过在组播路由器上静态配置SSM地址的映射规则，将IGMPv1和IGMPv2的报告报文中的（*，G）信息转化为对应的（S，G）信息，向运行IGMPv1或IGMPv2的成员提供SSM服务。缺省情况下，SSM组地址范围为232.0.0.0～232.255.255.255。可以通过配置来扩展SSM组地址范围，配置方法请参见**（可选）配置SSM组策略**。

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 ssm-mapping enable**，使能IGMP SSM Mapping功能。

缺省情况下，接口未使能IGMP SSM Mapping。

为保证接口网段内运行任意版本IGMP的成员主机都能得到SSM服务，建议在路由器的接口上运行IGMPv3。

步骤4 执行命令**quit**，返回系统视图。

步骤5 执行命令**igmp** [**vpn-instance** *vpn-instance-name*]，进入IGMP视图。

步骤6 执行命令**ssm-mapping** *group-address* { *group-mask* | *group-mask-length* } *source-address*，配置组到源的SSM Mapping规则。

缺省情况下，设备上未配置SSM Mapping规则。

----结束

检查配置结果

配置IGMP SSM Mapping功能后，在任意视图下执行以下命令，可以查看配置的映射关系、接口上IGMP SSM Mapping是否使能。

- 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address* | **interface** *interface-type interface-number*]* **ssm-mapping** [**verbose**]，查看配置了映射规则的组播组信息。
- 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **ssm-mapping** { **group** [*group-address*] | **interface** [*interface-type interface-number*] }，查看配置的映射关系、接口上IGMP SSM Mapping是否使能。

2.10 配置 IGMP Limit

IGMP Limit提供了对组成员关系的个数限制功能。

前置任务

2.7 配置IGMP基本功能

背景信息

按照组播协议的规定，组播组成员可以在任意时间、任意位置加入或退出组播组，并且加入的组成员总数不受限制。但是当大量用户同时收看多套节目时，需要占用组播设备的大量带宽，可能会造成组播性能下降。为了避免这种情况的发生，可以在组播路由器上配置IGMP Limit功能，通过限制全局、单实例或接口下的组播组个数，使加入组播组的用户收看更加清晰稳定的节目。当组播路由器收到Report报文时，首先判断是否超过配置的个数限制，如果没有超过，才建立组成员关系，给用户转发该组的数据流。

设备全局的成员个数限制即对所有实例下表项总和进行限制。单实例的成员个数限制即对当前实例下表项总和进行限制。接口下的成员个数限制即对当前接口下表项总和进行限制。

组成员关系的计数规则为：

- 每个（*，G）组成员关系计为一个表项。
- 每个（S，G）源组成员关系计为一个表项。
- 使用IGMP SSM Mapping的每个（*，G）组成员关系计为一个表项，按照映射生成的（S，G）表项不进行计数。

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。

操作步骤

- 配置全局IGMP组成员关系个数限制
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**igmp global limit** *number*，配置全局IGMP组成员关系个数限制。
- 配置单实例IGMP组成员关系个数限制
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**igmp** [**vpn-instance** *vpn-instance-name*]，进入公网实例或VPN实例的IGMP视图。
  c. 执行命令**limit** *number*，配置当前实例中可以创建的IGMP组成员关系个数限制。
- 配置基于接口的IGMP组成员关系个数限制
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**igmp limit** *number* [**except** { *acl-number* | **acl-name** *acl-name* }]，配置当前接口上能够创建的组成员关系个数限制。

如果未使用**except**参数，则动态创建的所有组或源组成员关系都受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报告报文。创建通过ACL过滤的表项时不受IGMP表项最大个数限制。

----结束

检查配置结果

- 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]，查看接口上的IGMP配置和运行信息。

2.11 配置 IGMP Proxy 功能

在一些简单的树形网络拓扑中，与成员主机网段直连的组播设备上不需要运行复杂的组播路由协议（如PIM）。可以在这些设备上配置IGMP Proxy功能，使其代理上游接入设备和下游成员主机的功能，从而有效地节约网络带宽，减轻接入设备的处理压力。

前置任务

在配置IGMP Proxy功能之前，需完成以下任务：

- 配置单播路由协议，使各节点间IP路由可达。
- 全局使能组播路由功能。

配置流程

按如下配置顺序进行配置。

2.11.1 配置 IGMP Proxy 基本功能

背景信息

在一些简单的树型网络拓扑中，与用户网段直接相邻的组播路由器上并不需要运行复杂的组播路由协议（如PIM），而透传主机IGMP报文又会导致上游接入设备管理太多用户。此时可以通过在与用户网段直接相邻的组播路由器上配置IGMP Proxy（IGMP代理）功能，使其收集下游用户的IGMP成员报告/离开信息，将成员报告/离开信息汇聚后代理下游主机统一上送给接入设备，并维护组成员关系，基于组成员关系进行组播转发。在上游接入设备看来，配置了IGMP Proxy功能的组播路由器就是一台主机。

在IGMP代理设备的上游接口上配置IGMP Proxy功能，在下游接口上配置IGMP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**igmp proxy**，使能IGMP Proxy功能。

缺省情况下，接口上未使能IGMP Proxy功能。

----结束

2.11.2 （可选）配置 IGMP Proxy 备份功能

背景信息

通常情况下，当配置了IGMP Proxy的上游接口发生故障时，IGMP代理功能无法正常运行。此时，为了保证网络中IGMP业务的正常运行，可以在配置完IGMP Proxy上游接口后再为其配置一个IGMP Proxy备份接口。此后，当IGMP Proxy上游接口发生故障时，备份接口会自动接管IGMP代理业务，使业务能够自动恢复。

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 proxy backup**，配置接口成为IGMP Proxy备份接口。

缺省情况下，接口上的IGMP Proxy备份功能处于关闭状态。

----结束

2.11.3 （可选）配置 IGMP Proxy 与 NQA 联动功能

背景信息

IGMP Proxy本身并没有检测机制，如果组播链路发生了故障，无法保证及时进行主、备链路的切换，可能造成较长时间的组播业务中断。通过IGMP Proxy与NQA联动可以解决此问题。

IGMP Proxy与NQA测试例联动是利用NQA测试例检测端到端的链路状态。当NQA测试例检测到上游接口所在链路发生故障时，配置了IGMP Proxy备份功能的设备能够及时进行主、备链路的切换，从而避免通信长时间中断。

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**nqa test-instance** *admin-name test-name*，建立NQA测试例，并进入测试例视图。

步骤3 执行命令**test-type icmp**，配置测试例类型为ICMP。

步骤4 执行命令**destination-address ipv4** *ipv4-address*，配置目的地址。

步骤5 执行命令**quit**，返回系统视图。

步骤6 执行命令**interface** *interface-type interface-number*，进入上游接口视图。

步骤7 执行命令**igmp proxy track nqa** *admin-name test-name*，使能IGMP Proxy与NQA联动功能。

说明

以上给出了ICMP类型的NQA测试例的基本配置。NQA测试例的详细配置，请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列企业路由器配置指南-网络管理》中的“NQA配置”。

----结束

2.11.4 （可选）配置 SSM 组播组地址范围

背景信息

SSM的组地址缺省范围是232.0.0.0～232.255.255.255。通常情况下，IGMP Proxy设备接收到组地址属于该缺省范围的报告报文时，才会为组成员提供SSM服务。有时候希望限制SSM组地址范围，保证组播网络安全；或者SSM组地址不够用，需要扩展SSM组地址范围。此时，可以在IGMP Proxy设备上配置SSM组播组的地址范围，但需要确保网络内所有组播设备配置的SSM组地址范围都一致。

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

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

缺省情况下，IGMP Proxy SSM组地址范围是232.0.0.0/8。

----结束

2.11.5 （可选）配置源生存时间

背景信息

Proxy设备为每个（S，G）表项设立一个定时器，“源生存时间”就是Proxy设备上（S，G）表项的超时时间。

接口第一次收到组播源S发往组播组G的组播报文后，启动定时器。然后，每接收到组播源S发出的组播报文就重置定时器，如果接口在源生存时间内没有收到组播源S发出的组播报文，则认为组播源停止向组播组G发送组播数据，（S，G）表项失效。

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

步骤3 执行命令**proxy source-lifetime** *interval*，配置源生存时间。

缺省情况下，源生存时间为210秒。

----结束

2.11.6 （可选）配置源地址过滤

背景信息

某些情况下，IGMP代理设备需要对接收的组播数据报文的源进行限制。此时，可以配置源地址过滤策略，使IGMP代理设备根据组播源或源组对接收到的组播报文进行过滤。

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**proxy source-policy** { *acl-number* | **acl-name** *acl-name* }，配置Proxy设备根据组播源或源组过滤接收的组播数据报文。

缺省情况下，Proxy设备不根据组播源或源组过滤接收的组播数据报文。

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

源地址过滤策略对静态加入的组播组或组播源组不进行过滤。

----结束

2.11.7 检查配置 IGMP Proxy 功能的结果

前提条件

完成IGMP Proxy功能配置后，在任意视图下执行以下命令，可以查看IGMP Proxy的接口信息、IGMP Proxy代理组的信息以及IGMP Proxy路由表信息。

操作步骤

- 执行命令**display igmp proxy** [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface**，查看使能IGMP Proxy的接口信息。
- 执行命令**display igmp proxy** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] [**verbose**]，查看IGMP Proxy代理组的信息。
- 执行命令**display igmp proxy** [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **none** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]，查看IGMP Proxy路由表信息。

----结束

2.12 维护 IGMP

IGMP的维护包括：清除IGMP的组信息、清除IGMP报文统计信息、监控IGMP运行状况。

2.12.1 清除 IGMP 组信息

背景信息

注意

清除IGMP组信息后，可能导致组播成员无法正常接收组播数据，请慎用。

操作步骤

- 在用户视图下，执行命令**reset igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *group-mask* | *group-mask-length* }] [*source-address* [**mask** { *source-mask* | *source-mask-length* }]] } }，清除接口上动态加入的组播组。
- 在接口视图下，执行命令**undo igmp static-group** { **all** | *group-address* [**inc-step-mask** { *group-mask* | *group-mask-length* } **number** *group-number*] [**source** *source-address*] }，清除接口静态加入的组播组。
- 在用户视图下，执行命令**reset igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group ssm-mapping** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *group-mask* | *group-mask-length* }] } }，清除根据IGMP SSM Mapping规则建立的组播组。

----结束

2.12.2 清除 IGMP 报文统计信息

背景信息

需要查看某一时间段内IGMP控制报文的准确统计信息时，先执行以下命令将之前的统计信息清除，然后再查看报文统计信息。

注意

清除IGMP控制报文统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

- 在用户视图下执行命令**reset igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**interface** *interface-type interface-number*] [**message-type** { **query** | **report** }]，清除IGMP控制报文统计数。

----结束

2.12.3 监控 IGMP 运行状况

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解IGMP的运行状况。

操作步骤

- 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address* | **interface** *interface-type interface-number*]* [**verbose**]，查看动态加入IGMP组播组的成员信息。
- 执行以下命令，查看静态IGMP组播组的成员信息。
  - 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] **static** [**up** | **down**] [**verbose**]，查看状态是Up或Down并且静态加入组播组的接口信息。
  - 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] **static interface-number**，查看加入IGMP静态组播组的接口数量。
  - 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] **interface** *interface-type interface-number* **static** [**verbose**]，查看指定接口上静态加入的组播组信息。
  - 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group static interface** *interface-type interface-number* **entry-number**，查看指定接口上加入的IGMP静态组播组数量。
- 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]，查看接口上IGMP配置和运行信息。
- 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }]]* [**static**] [**outgoing-interface-number** [*number*]]，查看IGMP路由表信息。
- 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address* | **interface** *interface-type interface-number*]* **ssm-mapping** [**verbose**]，查看配置了映射规则的组播组信息。
- 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **ssm-mapping** { **group** [*group-address*] | **interface** [*interface-type interface-number*] }，查看配置的映射关系、接口上IGMP SSM Mapping是否使能。
- 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**interface** *interface-type interface-number*] [**message-type** { **query** | **report** }]，查看IGMP报文统计计数。
- 执行以下命令，查看IGMP无效报文的统计信息及详细信息。
  - 执行命令**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** [**interface** *interface-type interface-number* | **message-type** { **leave** | **query** | **report** }]*，查看无效IGMP报文的统计信息。
  - 执行命令**display igmp invalid-packet** [*packet-number*] **verbose**，查看最近接收到的IGMP无效报文的详细信息。

----结束

2.13 IGMP 配置举例

针对如何在组播网络中配置IGMP基本功能、静态加入组、IGMP SSM Mapping、IGMP Limit、IGMP Proxy，分别提供配置举例。

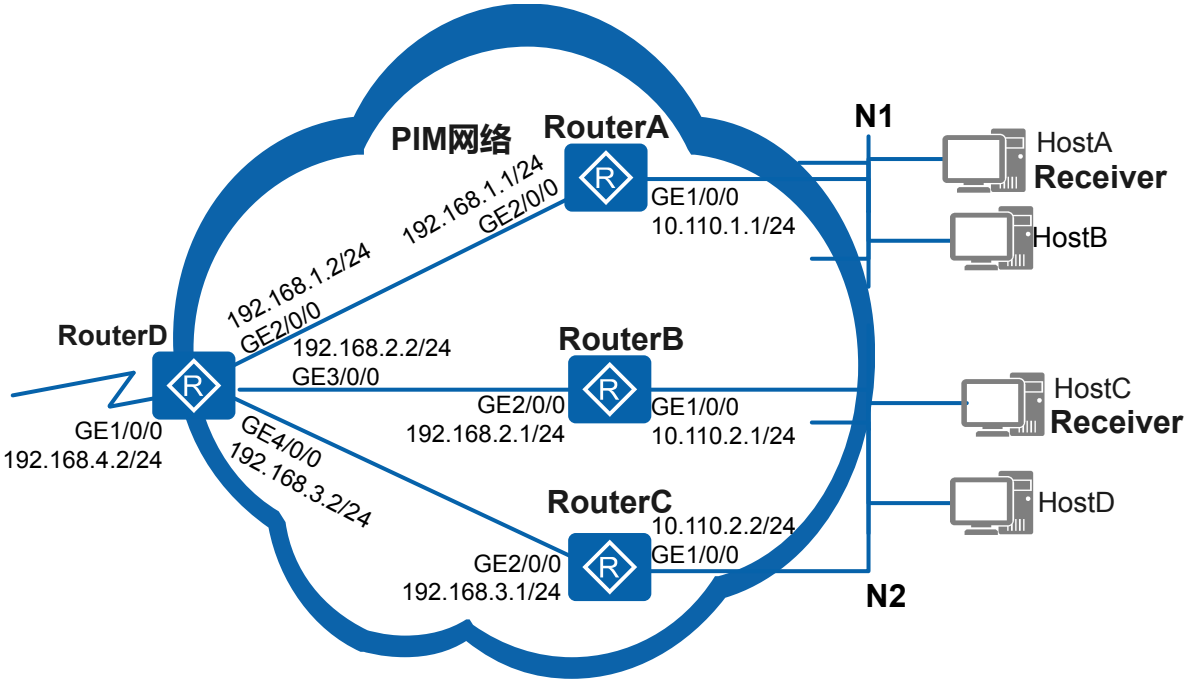
2.13.1 配置 IGMP 基本功能示例

组网需求

如图2-18所示，网络中的不同用户群组成N1和N2两个末梢网络。PIM网络中的RouterA连接用户网段N1，RouterB和RouterC连接用户网段N2。该PIM网络中传播视频信息使用的组播组地址为225.1.1.1～225.1.1.5。

N1中的HostA和N2中的HostC都希望通过组播方式接收视频信息。接收者HostA只购买了组播组225.1.1.1对应的节目，HostC则购买了所有组播组对应的节目。因此，需要在Router上进行相关配置，使得HostA只能接收组播组225.1.1.1的视频信息，而HostC则没有限制。

图 2-18 配置 IGMP 的基本功能组网图



配置思路

通过在Router上配置IGMP的基本功能以及限制RouterA与N1网段相连接口加入的组播组范围，可以实现此需求。

1. 为了保证组播源的数据可以正确的转发到用户网段，需要配置网络中的单播路由协议，实现网络层互通。单播路由正常是组播路由协议正常工作的基础。

2. 为了实现用户通过组播方式接收视频信息，需要在各Router上配置基本组播功能，实现组播数据在网络中的转发。
3. 为了使HostA只接收组播组225.1.1.1的视频信息，需要对HostA能接收的组播数据进行限制。可以通过在RouterA与N1网段相连的接口上配置组播过滤策略，实现对组播数据的过滤。

操作步骤

步骤1 配置各Router接口的IP地址和单播路由协议。

按照图2-18配置各Router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，并且各Router之间能够借助单播路由协议实现动态路由更新。RouterB、RouterC和RouterD上的配置过程与RouterA上的配置相似，配置过程略，详见配置文件。

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

步骤2 使能IP组播路由功能，并在所有接口上使能PIM-SM功能。

在RouterA上使能IP组播路由功能，并在所有接口上使能PIM-SM功能。RouterB、RouterC和RouterD上的配置过程与此类似，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] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] pim sm
[RouterA-GigabitEthernet2/0/0] quit
```

步骤3 配置静态RP。

在RouterA上，配置RouterD的GE1/0/0为静态RP。RouterB、RouterC和RouterD上的配置过程与此类似，配置过程略，详见配置文件。

```
[RouterA] pim
[RouterA-pim] static-rp 192.168.4.2
[RouterA-pim] quit
```

步骤4 在RouterA、RouterB、RouterC成员端接口上使能IGMP功能。

在RouterA的GE1/0/0接口上使能IGMP功能。RouterB和RouterC上的配置过程与此类似，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5 配置RouterA的GE1/0/0接口只能加入组播组225.1.1.1。

先创建ACL，配置其规则为允许组播组225.1.1.1的报文通过，然后在RouterA的GE1/0/0接口上应用该策略。


```
[RouterA] acl number 2001
[RouterA-acl-basic-2001] rule permit source 225.1.1.1 0
[RouterA-acl-basic-2001] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] igmp group-policy 2001
[RouterA-GigabitEthernet1/0/0] quit
```

步骤6 验证配置结果。

通过**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。

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 of VPN-Instance: public net
 Gigabitethernet1/0/0(10.110.1.1):
  IGMP is enabled
  Current IGMP version is 2
  IGMP state: up
  IGMP group policy: 2001
  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: 10.110.1.1 (this router)
 Total 1 IGMP Group reported
```

可以看出，RouterA的GE1/0/0接口已经使能了IGMP，并且应用了acl number为2001的组播组过滤策略。还可以看出，GE1/0/0接口接收到了一个组播组的报告报文。

RouterB上的GE1/0/0接口上IGMP的显示信息如下：

```
<RouterB> display igmp interface gigabitethernet 1/0/0
Interface information of VPN-Instance: public net
 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
```

可以看到，RouterB是查询器，这是因为同一网段上组播路由器RouterB的GE1/0/0接口的IP地址较小。还可以看出，GE1/0/0接口接收到了两个组播组的报告报文。

通过**display pim routing-table**命令，可以查看各路由器的PIM-SM组播路由表。

在RouterB和RouterC所在的共享网段，RouterB竞选为组播数据的转发者。RouterB上PIM-SM组播路由表信息显示如下：

```
<RouterB> display pim routing-table
 VPN-Instance: public net
 Total 2 (*, G) entries; 2 (S, G) entries

 (*, 225.1.1.1)
     RP: 192.168.4.2
     Protocol: pim-sm, Flag: WC
     UpTime: 00:21:35
     Upstream interface: GigabitEthernet2/0/0
         Upstream neighbor: 192.168.2.2
```

```
        RPF prime neighbor: 192.168.2.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet1/0/0
            Protocol: igmp, UpTime: 00:21:35, Expires: -

(193.3.5.2, 225.1.1.1)
    RP: 192.168.4.2
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 00:42:46
    Upstream interface: GigabitEthernet2/0/0
        Upstream neighbor: 192.168.2.2
        RPF prime neighbor: 192.168.2.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet1/0/0
            Protocol: pim-sm, UpTime: 00:21:35, Expires: -

(*, 225.1.1.2)
    RP: 192.168.4.2
    Protocol: pim-sm, Flag: WC
    UpTime: 00:06:02
    Upstream interface: GigabitEthernet2/0/0
        Upstream neighbor: 192.168.2.2
        RPF prime neighbor: 192.168.2.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet1/0/0
            Protocol: igmp, UpTime: 00:06:02, Expires: -

(193.3.5.2, 225.1.1.2)
    RP: 192.168.4.2
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 00:15:12
    Upstream interface: GigabitEthernet2/0/0
        Upstream neighbor: 192.168.2.2
        RPF prime neighbor: 192.168.2.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet1/0/0
            Protocol: pim-sm, UpTime: 00:06:04, Expires: -
```

可以看出，RouterB上有(*, 225.1.1.1)和(193.3.5.2, 225.1.1.1)表项，还有(*, 225.1.1.2)和(193.3.5.2, 225.1.1.2)表项。这表明GE1/0/0加入了组播组225.1.1.1和225.1.1.2，并且能够接收到组播源193.3.5.2向这两个组播组发送的数据。

RouterA上PIM-SM组播路由表信息显示如下：

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

 (*, 225.1.1.1)
    RP: 192.168.4.2
    Protocol: pim-sm, Flag: WC
    UpTime: 00:21:35
    Upstream interface: GigabitEthernet2/0/0
        Upstream neighbor: 192.168.1.2
        RPF prime neighbor: 192.168.1.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet1/0/0
            Protocol: igmp, UpTime: 00:21:35, Expires: -

 (193.3.5.2, 225.1.1.1)
    RP: 192.168.4.2
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 00:42:46
```



```
    Upstream interface: GigabitEthernet2/0/0
        Upstream neighbor: 192.168.1.2
        RPF prime neighbor: 192.168.1.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet1/0/0
            Protocol: pim-sm, UpTime: 00:21:35, Expires: -
```

可以看出，RouterA上只有(*, 225.1.1.1)和(193.3.5.2, 225.1.1.1)表项，这是因为RouterA的GE1/0/0接口上配置了组播组过滤策略。

----结束

配置文件

- RouterA的配置文件

```
#
 sysname RouterA
#
multicast routing-enable
#
acl number 2001
 rule 5 permit source 225.1.1.1 0
#
interface GigabitEthernet1/0/0
 ip address 10.110.1.1 255.255.255.0
 pim sm
 igmp enable
 igmp group-policy 2001
#
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 192.168.4.2
#
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 192.168.4.2
```



```
#
return
```

- RouterC的配置文件

```
#
 sysname RouterC
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 10.110.2.2 255.255.255.0
 pim sm
 igmp enable
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
pim
 static-rp 192.168.4.2
#
return
```

- RouterD的配置文件

```
#
 sysname RouterD
#
multicast routing-enable
#
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 192.168.2.2 255.255.255.0
 pim sm
#
interface GigabitEthernet4/0/0
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
 static-rp 192.168.4.2
#
return
```

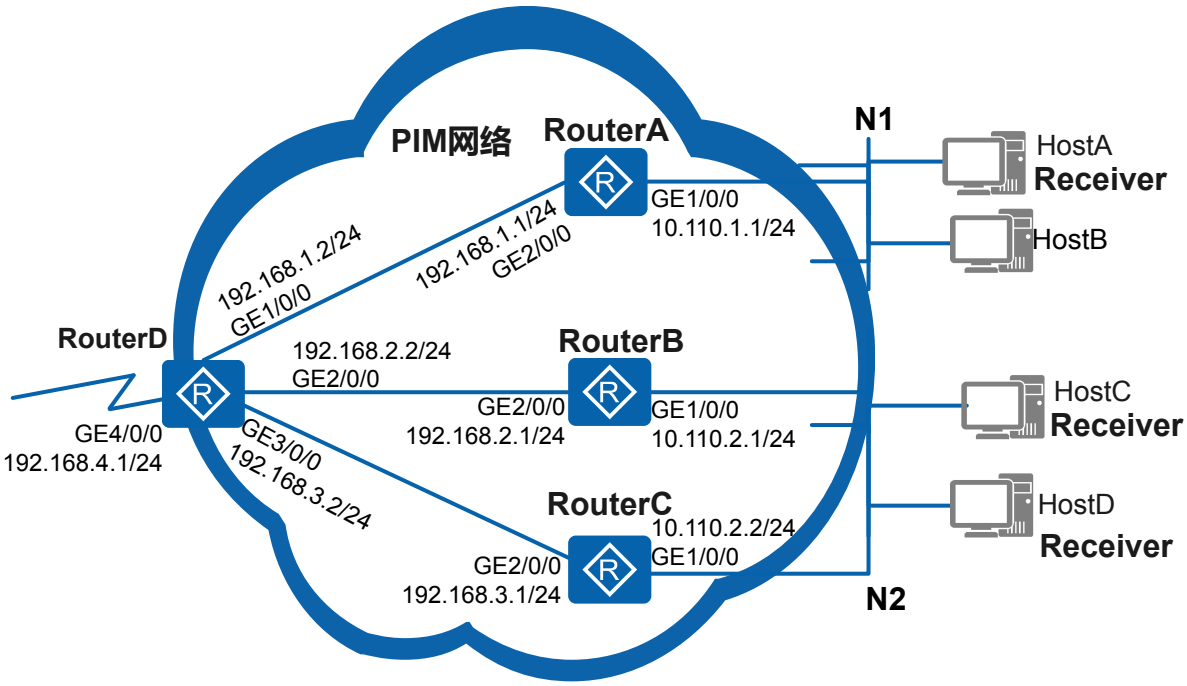
2.13.2 配置静态加入组播组示例

组网需求

如图2-19所示，网络中的不同用户群组成N1和N2两个末梢网络。PIM网络中的RouterA连接用户网段N1，RouterB和RouterC连接用户网段N2。该PIM网络中传播视频信息使用的组播组地址为225.1.1.1～225.1.1.5。

N1中的HostA和N2中的HostC、HostD都希望通过组播方式接收视频信息。其中接收者HostA希望长期稳定地接收组播组225.1.1.1的数据，HostC和HostD对组播组没有这样的需求。

图 2-19 配置 IGMP 静态组播组组网图



配置思路

配置RouterA与N1网段相连的接口静态加入组播组，可以实现此需求。

1. 为了保证组播源的数据可以正确的转发到用户网段，需要配置网络中的单播路由协议，实现网络层互通。单播路由正常是组播路由协议正常工作的基础。
2. 为了实现用户通过组播方式接收视频信息，需要在各Router上配置基本组播功能，实现组播数据在网络中的转发。
3. 为了使价值用户HostA可以稳定接收225.1.1.1的数据，需要在RouterA与N1网段相连的接口上配置静态加入组播组。

操作步骤

步骤1 配置各Router接口的IP地址和单播路由协议。

按照图2-19配置各Router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，并且各Router之间能够借助单播路由协议实现动态路由更新。RouterB、RouterC和RouterD上的配置过程与RouterA上的配置相似，配置过程略，详见配置文件。


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

步骤2 使能IP组播路由功能，并在所有接口上使能PIM-SM功能。

在RouterA上使能IP组播路由功能，并在所有接口上使能PIM-SM功能。RouterB、RouterC和RouterD上的配置过程与此类似，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] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] pim sm
[RouterA-GigabitEthernet2/0/0] quit
```

步骤3 配置静态RP。

在RouterA上，配置RouterD的GE4/0/0为静态RP。RouterB、RouterC和RouterD上的配置过程与此类似，配置过程略，详见配置文件。

```
[RouterA] pim
[RouterA-pim] static-rp 192.168.4.1
[RouterA-pim] quit
```

步骤4 在RouterA、RouterB、RouterC成员端接口上使能IGMP功能。

在RouterA的GE1/0/0接口上使能IGMP功能。RouterB和RouterC上的配置过程与此类似，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5 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下的用户能长期稳定地接收发往组播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6 验证配置结果。

通过**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 of VPN-Instance: public net
 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
```

可以看出，RouterB的GE1/0/0接口已经使能了IGMP。

通过**display pim routing-table**命令，可以查看RouterA的接口GE1/0/0是否已经静态加入组播组225.1.1.1。显示信息如下：

```
<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: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/0
             Protocol: static igmp, UpTime: 00:12:17, Expires: -
```

可以看出，RouterA上有（*，225.1.1.1）表项，且下游接口是GigabitEthernet1/0/0，协议类型“static igmp”，表明GigabitEthernet1/0/0静态加入组播组225.1.1.1配置成功。若RouterA的接口GE1/0/0未使能IGMP，则此处的协议类型为“static”。

----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
```

- RouterD的配置文件

```
#
 sysname RouterD
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 192.168.3.2 255.255.255.0
 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 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
```



```
 network 192.168.4.0 0.0.0.255
#
pim
 static-rp 192.168.4.1
#
return
```

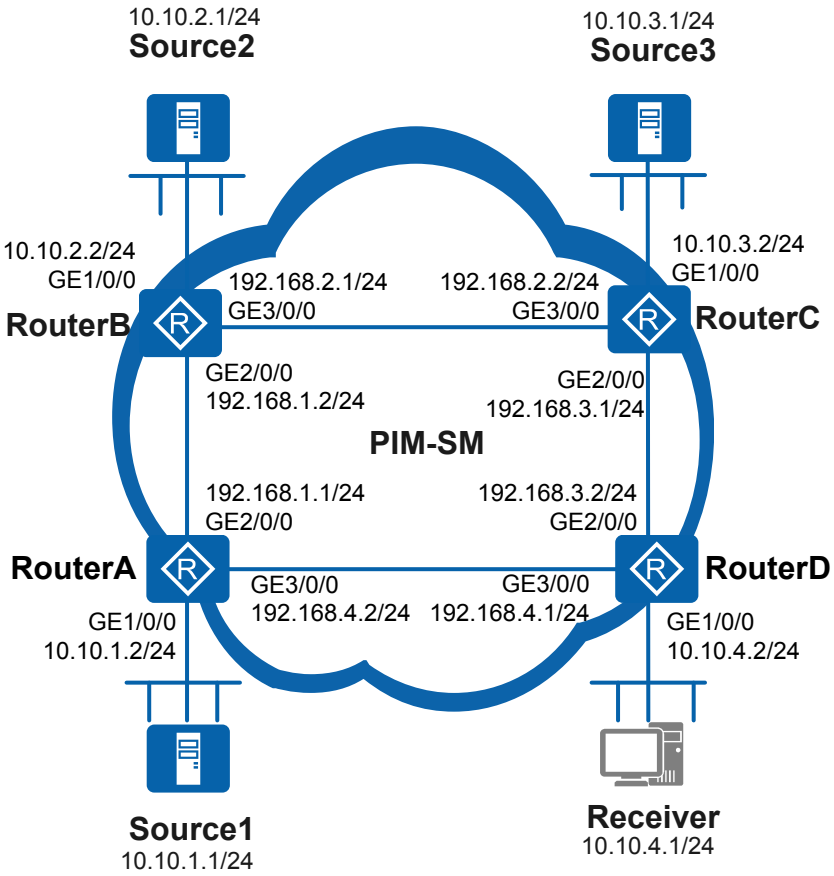
2.13.3 配置 IGMP SSM Mapping 功能示例

组网需求

如图2-20所示，该PIM网络运行PIM-SM协议，并使用SSM模式为组成员提供组播服务。与成员主机Receiver网段相连的RouterD的接口GE1/0/0上运行IGMPv3；Receiver运行IGMPv2，并且不能升级到IGMPv3，因此该主机在加入组播组时无法指定组播源。当前网络中的SSM组地址范围是232.1.1.0/24，Source1、Source2和Source3都向该范围内的组播组发送组播数据。

Receiver要求通过一定的配置能够获得SSM服务，只接收来自Source1和Source3的组播数据，阻止来自Source2的组播数据。

图 2-20 配置 IGMP SSM Mapping 功能组网图



配置思路

通过在RouterD上配置IGMP SSM Mapping功能，可以实现此需求。

1. 为了保证组播源的数据可以正确的转发到用户网段，需要配置网络中的单播路由协议，实现网络层互通。单播路由正常是组播路由协议正常工作的基础。
2. 为了实现用户通过组播方式接收视频信息，需要在各Router上配置基本组播功能，实现组播数据在网络中的转发。
3. 为了使Receiver可以接收指定组播源的数据，需要在RouterD上使能IGMP SSM Mapping功能并配置Mapping规则。

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2-20配置各Router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，并且各Router之间能够借助单播路由协议实现动态路由更新。RouterB、RouterC和RouterD上的配置过程与RouterA上的配置相似，配置过程略，详见配置文件。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 10.10.1.2 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 192.168.4.2 24
[RouterA-GigabitEthernet3/0/0] quit
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.10.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.4.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

步骤2 使能IP组播路由功能，并在所有接口上使能PIM-SM功能。

在RouterA上使能IP组播路由，并在所有接口上使能PIM-SM功能。RouterB、RouterC和RouterD上的配置过程与此类似，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] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] pim sm
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] pim sm
[RouterA-GigabitEthernet3/0/0] quit
```

步骤3 在RouterD的成员端接口上使能IGMP，配置版本为IGMPv3。

在RouterD的成员端接口GE1/0/0上使能IGMP，并配置版本为IGMPv3。

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

步骤4 使能成员端接口的IGMP SSM Mapping功能。

在RouterD的GE1/0/0上使能IGMP SSM Mapping功能。


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

步骤5 在所有Router上配置SSM组播组地址范围。

在RouterA上配置SSM组播组地址范围为232.1.1.0/24。RouterB、RouterC和RouterD上的配置过程与RouterA上的配置类似，配置过程略，详见配置文件。

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

步骤6 在连接主机的RouterD上配置IGMP SSM Mapping的映射规则。

在RouterD上，将232.1.1.0/24范围内的组播组映射到Source1和Source3。

```
[RouterD] igmp
[RouterD-igmp] ssm-mapping 232.1.1.0 24 10.10.1.1
[RouterD-igmp] ssm-mapping 232.1.1.0 24 10.10.3.1
[RouterD-igmp] quit
```

步骤7 验证配置结果。

通过**display igmp ssm-mapping group**命令可以查看RouterD上组播源和组播组的映射关系。

```
<RouterD> display igmp ssm-mapping group
IGMP SSM-Mapping conversion table of VPN-Instance: public net
 Total 2 entries    2 entries matched

 00001. (10.10.1.1, 232.1.1.0/24)

 00002. (10.10.3.1, 232.1.1.0/24)

 Total 2 entries matched
```

可以看出，232.1.1.0/24范围内的组播组已经映射到Source1和Source3。

通过**display igmp group ssm-mapping**命令可以查看RouterD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 of VPN-Instance: public net

 Limited entry of this VPN-Instance: -
 GigabitEthernet1/0/0(10.10.4.2):
  Total 1 IGMP SSM-Mapping Group reported
   Group Address   Last Reporter   Uptime      Expires
   232.1.1.1       10.10.4.1       00:01:44    00:00:26
```

可以看出，Receiver已经加入组232.1.1.1。

通过使用**display pim routing-table**命令可以查看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 2 (S, G) entries

 (10.10.1.1, 232.1.1.1)
```



```
    Protocol: pim-ssm, Flag: SG_RCVR
    UpTime: 00:19:40
    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: 00:19:40, Expires: -

(10.10.3.1, 232.1.1.1)
    Protocol: pim-ssm, Flag: SG_RCVR
    UpTime: 00:19:40
    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: 00:19:40, Expires: -
```

可以看出，组播源10.10.1.1和10.10.3.1向组播组232.1.1.1发送组播数据，RouterD分别从接口GE3/0/0和GE2/0/0接收以上两个组播源的数据。

----结束

配置文件

- RouterA的配置文件

```
#
 sysname RouterA
#
multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 10.10.1.2 255.255.255.0
 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 10.10.1.0 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 232.1.1.0 0.0.0.255
```



```
#
interface GigabitEthernet1/0/0
 ip address 10.10.2.2 255.255.255.0
 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 10.10.2.0 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 232.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 10.10.3.2 255.255.255.0
 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 10.10.3.0 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

```
#
 sysname RouterD
#
multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 10.10.4.2 255.255.255.0
 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
#
ospf 1
 area 0.0.0.0
  network 10.10.4 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
igmp
 ssm-mapping 232.1.1.0 255.255.255.0 10.10.1.1
 ssm-mapping 232.1.1.0 255.255.255.0 10.10.3.1
#
pim
 ssm-policy 2000
#
return
```

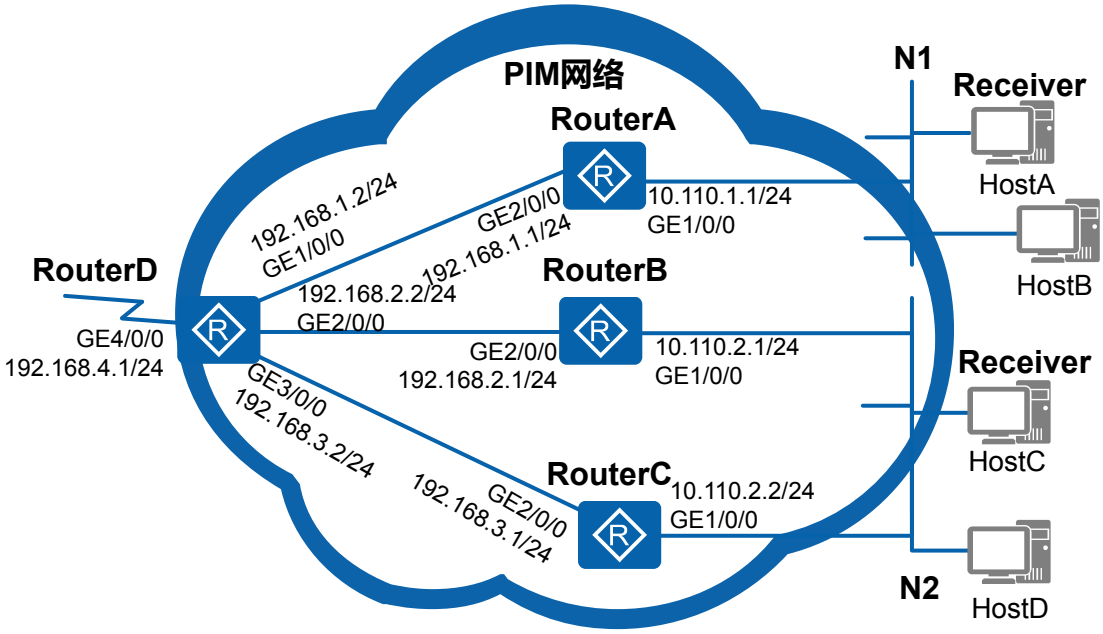
2.13.4 配置 IGMP Limit 示例

组网需求

如图2-21所示，该网络中有大量成员主机通过组播方式接收视频节目。在黄金时段，网络中会有大量用户同时收看多套视频节目，占用设备的大量带宽，造成设备性能下降，导致成员主机接收组播数据的稳定性变差。

网络中需要对成员主机点播的节目数量进行限制，当节目点播数量达到限制值时不允许再点播新的节目，保证用户已订购节目的接收质量。同时，与RouterA相连网段的HostA为价值用户，该用户订购了一个长期的组地址225.1.1.3的节目，他要求任意时刻都可以无阻塞地接收到来自225.1.1.3的视频数据。

图 2-21 配置 IGMP Limit 组网图



配置思路

通过在RouterA与成员主机网段相连的接口上将225.1.1.3配置为静态组播组，同时配置IGMP Limit功能对组成员关系的个数进行限制，可以实现此需求。

1. 为了保证组播源的数据可以正确的转发到用户网段，需要配置网络中的单播路由协议，实现网络层互通。单播路由正常是组播路由协议正常工作的基础。
2. 为了实现用户通过组播方式接收视频信息，需要在各Router上配置基本组播功能，实现组播数据在网络中的转发。
3. 为了使价值用户HostA在任意时刻都可以无阻塞地接收到来自225.1.1.3的视频数据，需要在RouterA连接该用户网段的接口上配置静态加入组播组。
4. 为了对成员主机点播的节目数量进行限制，实现组播用户点播的灵活控制，需要在各Router上配置IGMP组成员关系个数限制。配置的限制值不仅对静态加入的组播组没有影响，还能保证该组的接收质量。

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2-21配置各Router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，并且各Router之间能够借助单播路由协议实现动态路由更新。RouterB、RouterC和RouterD上的配置过程与RouterA上的配置相似，配置过程略，详见配置文件。

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

步骤2 使能IP组播路由功能，并在所有接口上使能PIM-SM功能。

在RouterA上使能组播功能，并在所有接口上使能PIM-SM功能。RouterB、RouterC和RouterD上的配置过程与此类似，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] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] pim sm
[RouterA-GigabitEthernet2/0/0] quit
```

步骤3 配置静态RP。

在RouterA上配置静态RP。配置RouterD上GE4/0/0接口的IP地址作为该PIM网络的静态RP地址。RouterB、RouterC和RouterD上的配置过程与此类似，配置过程略，详见配置文件。


```
[RouterA] pim
[RouterA-pim] static-rp 192.168.4.1
[RouterA-pim] quit
```

步骤4 在RouterA、RouterB、RouterC的成员端接口使能IGMP功能。

在RouterA的GE1/0/0接口使能IGMP。RouterB和RouterC的配置与此类似，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5 配置RouterA的GE1/0/0接口静态加入组播组。

将RouterA的GE1/0/0接口静态加入组播组225.1.1.3，使接口GE1/0/0下的用户能长期稳定地接收发往组播225.1.1.3的数据。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] igmp static-group 225.1.1.3
[RouterA-GigabitEthernet1/0/0] quit
```

步骤6 在连接成员主机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
```

配置物理接口GE1/0/0接口下总共可以创建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，详见配置文件。

步骤7 验证配置结果。

通过**display igmp interface**命令可以查看路由器接口上IGMP的配置和运行情况。例如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 of VPN-Instance: public net
 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)
 Total 1 IGMP Group reported
```

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。

通过**display igmp group interface gigabitethernet 1/0/0 static verbose**命令可以查看IGMP静态组播组的加入接口详细信息。


```
<RouterA> display igmp group interface gigabitethernet 1/0/0 static verbose
Static join group information of VPN-Instance: public net
 Total 1 entry
  00001.(*, 225.1.1.3)
      1.GigabitEthernet1/0/0
          State:             UP
          Reference Count:   1
          Multicast Boundary:NO
          Outgoing Interface:NO
```

可以看到，RouterA的GE1/0/0已经静态加入组播组225.1.1.3。

通过**display pim routing-table**命令，可以查看各PIM-SM组播路由表。

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

 (*, 225.1.1.3)
     RP: 192.168.4.1
     Protocol: pim-sm, Flag: WC
     UpTime: 00:21:35
     Upstream interface: GigabitEthernet2/0/0
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/0
             Protocol: static igmp, UpTime: 00:21:35, Expires: -

 (193.3.5.2, 225.1.1.3)
     RP: 192.168.4.1
     Protocol: pim-sm, Flag: SPT ACT
     UpTime: 00:42:46
     Upstream interface: GigabitEthernet2/0/0
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/0
             Protocol: pim-sm, UpTime: 00:21:35, Expires: -
```

可以看出，RouterA有(*, 225.1.1.3)和(193.3.5.2, 225.1.1.3)表项，这表明GE1/0/0加入了组播组225.1.1.3，并且能够接收到组播源193.3.5.2发往225.1.1.3的数据。

----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 225.1.1.3
#
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
#
pim
 static-rp 192.168.4.1
#
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
#
pim
 static-rp 192.168.4.1
#
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
```



```
#
pim
 static-rp 192.168.4.1
#
return
```

- RouterD的配置文件

```
#
 sysname RouterD
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface GigabitEthernet2/0/0
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface GigabitEthernet3/0/0
 ip address 192.168.3.2 255.255.255.0
 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 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
 static-rp 192.168.4.1
#
return
```

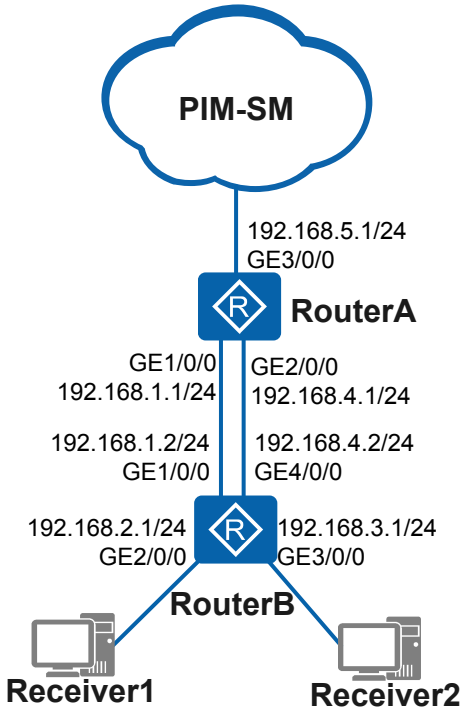
2.13.5 配置 IGMP Proxy 示例

组网需求

如图2-22所示，核心网络中运行PIM-SM，RouterA连接核心网络和三层设备RouterB，RouterB连接用户网段且没有运行PIM协议。

该网段有大量用户希望通过组播方式收看视频节目。如果RouterB透传成员主机发送的IGMP协议报文，会造成RouterA和RouterB之间的流量过大，增加RouterA的处理压力，进而影响到用户收看节目的质量。用户要求通过配置避免这种情况。

图 2-22 配置 IGMP Proxy 组网图



配置思路

通过在RouterB上配置IGMP Proxy功能可以缓解RouterA对IGMP协议报文的处理压力。

1. 为了保证组播源的数据可以正确的转发到用户网段，需要配置网络中的单播路由协议，实现网络层互通。单播路由正常是组播路由协议正常工作的基础。
2. 为了实现用户通过组播方式接收视频信息，需要在各Router上配置基本组播功能，实现组播数据在网络中的转发。
3. 为了实现RouterB对上游接入设备RouterA和下游成员主机的代理功能，需要在RouterB的GE1/0/0接口上配置IGMP Proxy功能，在RouterB与成员主机网段相连的接口上使能IGMP。
4. 为了保障IGMP Proxy功能的正常运行，防止因上游接口故障而导致的业务中断，可以在RouterB的GE4/0/0接口上配置IGMP Proxy备份功能。
5. 为了保证（S，G）表项的有效性，可以在RouterB上配置合适的源生存时间。

操作步骤

步骤1 配置各Router接口的IP地址和单播路由协议。

按照图2-22配置各Router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，并且各Router之间能够借助单播路由协议实现动态路由更新。RouterB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。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 24
```



```
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 192.168.4.1 24
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 192.168.5.1 24
[RouterA-GigabitEthernet3/0/0] quit
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.4.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.5.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

步骤2 在RouterA上使能IP组播路由功能、PIM-SM功能和IGMP功能。

在RouterA上使能IP组播路由功能，并在GE3/0/0接口上使能PIM-SM。配置GE3/0/0为C-BSR和C-RP。

```
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] pim sm
[RouterA-GigabitEthernet3/0/0] quit
[RouterA] pim
[RouterA-pim] c-bsr gigabitethernet 3/0/0
[RouterA-pim] c-rp gigabitethernet 3/0/0
[RouterA-pim] quit
```

在RouterA的GE1/0/0和GE2/0/0接口上使能IGMP功能，并配置IGMP版本为v3。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] igmp enable
[RouterA-GigabitEthernet1/0/0] igmp version 3
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] igmp enable
[RouterA-GigabitEthernet2/0/0] igmp version 3
[RouterA-GigabitEthernet2/0/0] quit
```

步骤3 在IGMP Proxy路由器RouterB上使能IP组播路由功能和IGMP功能。

在RouterB上使能组播功能，并在GE2/0/0和GE3/0/0接口上使能IGMP功能，配置IGMP版本为v3。

```
[RouterB] multicast routing-enable
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] igmp enable
[RouterB-GigabitEthernet2/0/0] igmp version 3
[RouterB-GigabitEthernet2/0/0] quit
[RouterB] interface gigabitethernet 3/0/0
[RouterB-GigabitEthernet3/0/0] igmp enable
[RouterB-GigabitEthernet3/0/0] igmp version 3
[RouterB-GigabitEthernet3/0/0] quit
```

步骤4 在IGMP Proxy路由器RouterB上游接口上使能IGMP Proxy基本功能。

在RouterB的GE1/0/0接口上使能IGMP Proxy基本功能，并配置IGMP健壮系数为3。

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] igmp proxy
[RouterB-GigabitEthernet1/0/0] igmp version 3
[RouterB-GigabitEthernet1/0/0] igmp robust-count 3
[RouterB-GigabitEthernet1/0/0] quit
```

步骤5 在IGMP Proxy路由器RouterB备份接口上使能IGMP Proxy备份功能。

在RouterB的GE4/0/0接口上使能IGMP Proxy备份功能。


```
[RouterB] interface gigabitethernet 4/0/0
[RouterB-GigabitEthernet4/0/0] igmp proxy backup
[RouterB-GigabitEthernet4/0/0] igmp version 3
[RouterB-GigabitEthernet4/0/0] quit
```

步骤6 在IGMP Proxy路由器RouterB的IGMP视图下配置源生存时间。

在RouterB的IGMP视图下配置源生存时间为300秒。

```
[RouterB] igmp
[RouterB-igmp] proxy source-lifetime 300
[RouterB-igmp] quit
```

步骤7 验证配置结果。

通过使用**display igmp proxy interface**命令可以查看路由器使能IGMP Proxy的接口信息。在RouterB上查看使能IGMP Proxy的接口信息如下：

```
[RouterB] display igmp proxy interface
Interface information of VPN-Instance: public net
 GigabitEthernet1/0/0(192.168.1.2):
   IGMP proxy is enabled
   Current IGMP proxy version (negotiated) is 3
   Current IGMP proxy version (configured) is 3
   IGMP proxy state: up
   Value of query interval for IGMP (negotiated): 60 s
   Value of query interval for IGMP (configured): 60 s
   Value of querier present timeout for IGMPv1: off
   Value of querier present timeout for IGMPv2: off
   Value of querier present timeout for IGMPv3: 124s
   General query response expiry: off
   Querier for IGMP: 192.168.1.1
   Robustness (negotiated): 3
   Robustness (configured): 3
   Require-router-alert: disabled
   Send-router-alert: enabled
   Ip-source-policy: disabled
   Query Ip-source-policy: disabled

 GigabitEthernet4/0/0(192.168.4.2):
   IGMP proxy backup is enabled
   Current IGMP proxy version (negotiated) is 3
   Current IGMP proxy version (configured) is 3
   IGMP proxy state: up
   Value of query interval for IGMP (negotiated): 60 s
   Value of query interval for IGMP (configured): 60 s
   Value of querier present timeout for IGMPv1: off
   Value of querier present timeout for IGMPv2: off
   Value of querier present timeout for IGMPv3: 124s
   General query response expiry: off
   Querier for IGMP: 192.168.4.1
   Robustness (negotiated): 2
   Robustness (configured): 2
   Require-router-alert: disabled
   Send-router-alert: enabled
   Ip-source-policy: disabled
   Query Ip-source-policy: disabled
```

可以看到，RouterB的接口GE1/0/0上使能了IGMP Proxy功能，接口GE4/0/0上使能了IGMP Proxy备份功能。

通过**display igmp proxy routing-table**命令可以查看路由器上IGMP Proxy路由表信息。下游用户Receiver1向上游发送组播源组（1.1.1.1，232.1.1.1）的加入，在RouterB上查看IGMP Proxy路由表信息如下：

```
[RouterB] display igmp proxy routing-table
Routing table of VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry
```



```
(1.1.1.1, 232.1.1.1)
    Flag: JOIN, UpTime: 01:38:45
    Upstream interface: GigabitEthernet1/0/0
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet2/0/0
            Protocol: igmp, UpTime: 01:38:45
```

可以看到，RouterB的Proxy路由表中有组播源组（1.1.1.1，232.1.1.1）的表项信息，说明下游用户Receiver1已经加入了组播源组（1.1.1.1，232.1.1.1）。

----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
 igmp enable
 igmp version 3
#
interface GigabitEthernet2/0/0
 ip address 192.168.4.1 255.255.255.0
 igmp enable
 igmp version 3
#
interface GigabitEthernet3/0/0
 ip address 192.168.5.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
  network 192.168.5.0 0.0.0.255
#
pim
 c-bsr GigabitEthernet3/0/0
 c-rp GigabitEthernet3/0/0
#
return
```

- RouterB的配置文件

```
#
 sysname RouterB
#
multicast routing-enable
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
 igmp version 3
 igmp robust-count 3
 igmp proxy
#
interface GigabitEthernet2/0/0
 ip address 192.168.2.1 255.255.255.0
 igmp enable
 igmp version 3
#
interface GigabitEthernet3/0/0
 ip address 192.168.3.1 255.255.255.0
 igmp enable
```



```
 igmp version 3
#
interface GigabitEthernet4/0/0
 ip address 192.168.4.2 255.255.255.0
 igmp version 3
 igmp proxy backup
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
igmp
 proxy source-lifetime 300
#
return
```

2.14 IGMP 常见配置错误

介绍了常见的配置错误的故障现象以及处理步骤。

2.14.1 IGMP 表项无法正常建立

故障现象

IGMP配置完成后，有成员主机需要接收组播组G的数据，离该成员主机最近的组播路由器上却没有生成IGMP组表项。

操作步骤

步骤1 检查成员主机点播的组地址是否为协议预留的组地址，范围为224.0.0.1～224.0.0.255。对于目的地址为这段地址的IGMP报告报文，设备不会生成IGMP组表项。

步骤2 执行**display interface** *interface-type interface-number*命令，查看与成员主机网段相连的接口状态是否Up。

如果接口状态Down，原因通常是接口连线不正确，或者接口上配置了**shutdown**命令，或者接口上没有配置正确的IP地址。

步骤3 执行**display current-configuration**命令，查看当前是否使能了IP组播路由功能。

如果显示信息中没有“multicast routing-enable”，则在系统视图下执行**multicast routing-enable**命令使能IP组播路由功能。

步骤4 执行**display current-configuration interface** *interface-type interface-number*命令，查看直连主机的接口是否使能了IGMP。

如果显示信息中没有“igmp enable”，说明未使能IGMP。在接口视图下执行**igmp enable**命令使能IGMP。

步骤5 执行**display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface** *interface-type interface-number*命令，检查接口上的IGMP配置是否正确。

- 接口上运行的IGMP版本“Current IGMP version”不能低于成员主机所使用的版本。

- “IGMP group policy”信息中如果显示配置了ACL规则，检查组播组是否在ACL限制的范围内。如果组播组不在ACL规则允许接收的范围内，需要修改该ACL规则，允许设备接收该组播组的报告报文。

----结束

2.14.2 配置 IGMP SSM Mapping 后没有生成（S，G）表项

故障现象

接口使能了SSM Mapping和IGMP，配置了SSM Mapping静态映射策略，也确实收到了IGMPv1或IGMPv2报告报文，组播转发表中却不存在指定了映射规则的（S，G）表项。

操作步骤

步骤1 检查（*，G）报告报文中的组G属不属于SSM组地址范围。

在PIM视图下使用**display this**命令查看当前配置。如果显示信息中出现了“ssm-policy”，则表明在该设备上重新定义了SSM组范围。

执行命令**display acl** { *acl-number* | **name** *acl-name* | **all** }，检查该ACL的配置信息。确保组G在SSM组地址范围内。默认情况下，SSM组范围为232.0.0.0～232.255.255.255。

----结束

2.15 IGMP 参考信息

介绍IGMP的相关RFC清单。

本特性的参考资料清单如下：

文档	描述	备注
RFC 1112	Host Extensions for IP Multicasting	-
RFC 2236	Internet Group Management Protocol, Version 2	-
RFC 3376	Internet Group Management Protocol, Version 3	-
RFC 3569	An Overview of Source-Specific Multicast (SSM)	-